



# A Baby Step–Giant Step Roadmap Algorithm for General Algebraic Sets

Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, Eric Schost

## ► To cite this version:

Saugata Basu, Marie-Françoise Roy, Mohab Safey El Din, Eric Schost. A Baby Step–Giant Step Roadmap Algorithm for General Algebraic Sets. Foundations of Computational Mathematics, 2014, 14 (6), pp.1117 - 1172. 10.1007/s10208-014-9212-1 . hal-01096209

**HAL Id: hal-01096209**

**<https://inria.hal.science/hal-01096209>**

Submitted on 17 Dec 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A BABY STEP-GIANT STEP ROADMAP ALGORITHM FOR GENERAL ALGEBRAIC SETS

S. BASU, M-F. ROY, M. SAFEY EL DIN, AND É. SHOST

ABSTRACT. Let  $R$  be a real closed field and  $D \subset R$  an ordered domain. We give an algorithm that takes as input a polynomial  $Q \in D[X_1, \dots, X_k]$ , and computes a description of a roadmap of the set of zeros,  $\text{Zer}(Q, R^k)$ , of  $Q$  in  $R^k$ . The complexity of the algorithm, measured by the number of arithmetic operations in the ordered domain  $D$ , is bounded by  $d^{O(k\sqrt{k})}$ , where  $d = \deg(Q) \geq 2$ . As a consequence, there exist algorithms for computing the number of semi-algebraically connected components of a real algebraic set,  $\text{Zer}(Q, R^k)$ , whose complexity is also bounded by  $d^{O(k\sqrt{k})}$ , where  $d = \deg(Q) \geq 2$ . The best previously known algorithm for constructing a roadmap of a real algebraic subset of  $R^k$  defined by a polynomial of degree  $d$  has complexity  $d^{O(k^2)}$ .

## 1. INTRODUCTION

The problem of designing efficient algorithms for deciding whether two points belong to the same semi-algebraically connected component of a semi-algebraic set, as well as counting the number of semi-algebraically connected components of a given semi-algebraic set  $S \subset R^k$  where  $R$  is a real closed field (for example the field of real numbers), is a very important problem in algorithmic semi-algebraic geometry.

The first algorithm for solving this problem [14] was based on the technique of cylindrical algebraic decomposition [6, 2], and consequently had doubly exponential complexity in  $k$ .

Algorithms with singly exponential complexity in  $k$  for solving this problem was first introduced by Canny in [5], and then successively completed and refined in [15, 11, 13, 12, 9, 10, 1]. They are all based on a geometric idea introduced by Canny, the construction of a one-dimensional s-a (i.e. semi-algebraic) subset of the given s-a set  $S$ , called a *roadmap of  $S$* , which has the property that it is non-empty and s-a connected inside every s-a (i.e. semi-algebraically) connected component of  $S$ .

In the papers mentioned above, the construction of a roadmap of a s-a set  $S$  depends on recursive calls to itself on several (in fact, singly exponentially many)  $(k - 1)$ -dimensional slices of  $S$ , each obtained by fixing the first coordinate. For

---

2010 *Mathematics Subject Classification.* Primary 14Q20; Secondary 14P05, 68W05.

*Key words and phrases.* Roadmaps, Real algebraic variety, Baby step-giant step.

Communicated by Teresa Krick.

The first author was supported in part by NSF grants CCF-0915954, CCF-1319080 and DMS-1161629. The first and the second authors did part of the work during a research stay in Oberwolfach as part of the Research in Pairs Programme. The third author is member of Institut Universitaire de France and supported by the French National Research Agency EXACTA grant (ANR-09-BLAN-0371-01) and GeoLMI grant (ANR-2011-BS03-011-06). The fourth author was supported by an NSERC Discovery Grant and by the Canada Research Chairs program.

constructing the roadmap of a real algebraic variety defined by a polynomial  $Q \in \mathbb{R}[X_1, \dots, X_k]$  with  $\deg(Q) \leq d$ , this technique gave an algorithm with complexity  $d^{O(k^2)}$ . The exponent in the upper bound on the complexity,  $O(k^2)$ , is due to the fact that the depth of the recursion in these algorithms could be as large as  $k$ . This exponent is not satisfactory since the total number of s-a connected components is  $(O(d))^k$  and so there is room for trying to improve it. However, this has turned out to be a rather difficult problem with no progress until very recently.

A new construction for computing roadmaps, with an improved recursive scheme of baby step - giant step type, has been proposed, and applied successfully in the case of smooth bounded real algebraic hypersurfaces in [8]. In this new recursive scheme, the dimension drops by  $\sqrt{k}$  in each recursive call. As a result, the depth of the recursive calls in this new algorithm is at most  $\sqrt{k}$ , and consequently the algorithm has a complexity of  $d^{O(k\sqrt{k})}$ . The proof of correctness of the algorithm in [8] depends on certain results from commutative algebra and complex algebraic geometry, in order to prove smoothness of polar varieties corresponding to generic projections of a non-singular hypersurface. Choosing generic coordinates in the algorithm is necessary since the non-singularity of polar varieties does not hold for all projections, but only for a Zariski-dense set of projections. This is an important restriction, since there is no known method for making such a choice of generic coordinates deterministically within this improved complexity bound. As a result, the authors obtain a randomized (rather than a deterministic) algorithm for computing roadmaps: there might be cases where the algorithm terminates and gives a wrong result.

In contrast to these techniques which depend on complex algebraic geometry, the algorithm for constructing roadmaps described in [2] depends mostly on arguments which are semi-algebraic in nature. The greater flexibility of semi-algebraic geometry (as opposed to complex geometry) makes it possible to avoid genericity requirements for coordinates. More precisely, we apply the technique used in [2] to make an infinitesimal deformation of the given variety so that the original coordinates are good. Since the infinitesimal deformation uses only one infinitesimal, it does not affect the asymptotic complexity class of the algorithm.

The goal of this paper is to obtain a *deterministic algorithm* for computing the roadmap of a *general algebraic set*, combining a baby step - giant step recursive scheme similar to that used in [8] and extending techniques coming from [2].

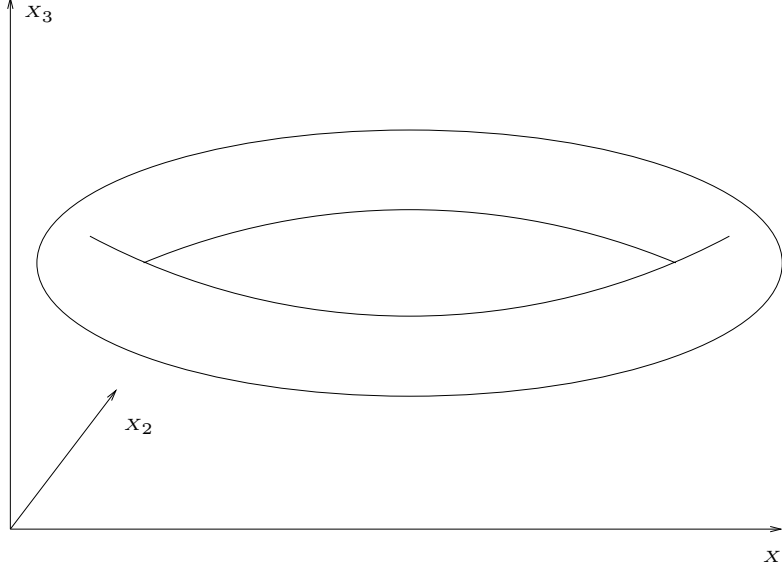
We start by recalling the precise definition of what is meant by a roadmap.

**Definition 1.1.** Let  $S \subset \mathbb{R}^k$  be a s-a set. A *roadmap* for  $S$  is a s-a set  $\text{RM}(S)$  of dimension at most one contained in  $S$  which satisfies the following roadmap conditions:

- (1)  $\text{RM}_1$  For every s-a connected component  $C$  of  $S$ ,  $C \cap \text{RM}(S)$  is s-a connected.
- (2)  $\text{RM}_2$  For every  $x \in \mathbb{R}$  and for every s-a connected component  $C'$  of  $S_x$ ,  $C' \cap \text{RM}(S) \neq \emptyset$ , where we denote by  $S_x$  the set  $S \cap \pi_1^{-1}(x)$  for  $x \in \mathbb{R}$ , with  $\pi_1 : \mathbb{R}^k \rightarrow \mathbb{R}$  the projection map onto the first coordinate.

Let  $\mathcal{M} \subset \mathbb{R}^k$  be a finite set of points. A roadmap for  $(S, \mathcal{M})$  is a s-a set  $\text{RM}(S, \mathcal{M})$  such that  $\text{RM}(S, \mathcal{M})$  is a roadmap of  $S$  and  $\mathcal{M} \subset \text{RM}(S, \mathcal{M})$ .

We illustrate this definition by the picture of a torus in  $\mathbb{R}^3$  and a roadmap of it.

FIGURE 1. Torus in  $\mathbb{R}^3$ 

The main result of the paper is the following theorem. The notion of real univariate representations used in the following statements to represent finite sets of point in  $\mathbb{R}^k$  is explained in Section 4.

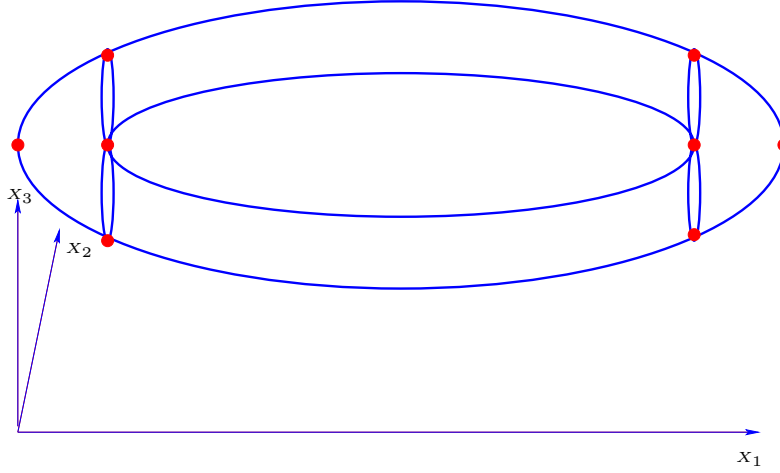
**Theorem 1.2.** *Let  $Z \subset \mathbb{R}^k$  be an algebraic set defined as the set of zeros of a polynomial of degree at most  $d \geq 2$  in  $k$  variables with coefficients in an ordered domain  $D$  contained in a real closed field  $\mathbb{R}$ .*

- a) *There exists an algorithm for constructing a roadmap for  $Z$  using  $d^{O(k\sqrt{k})}$  arithmetic operations in  $D$ .*
- b) *Moreover, there exists an algorithm that given a finite set of points  $\mathcal{M}_0 \subset Z$ , with cardinality  $\delta$ , and described by real univariate representations of degree at most  $d^{O(k)}$ , constructs a roadmap for  $(Z, \mathcal{M}_0)$  using  $\delta^{O(1)}d^{O(k\sqrt{k})}$  arithmetic operations in  $D$ .*

The following corollary is an immediate consequence of b).

**Corollary 1.3.** *Let  $Z \subset \mathbb{R}^k$  be an algebraic set defined as the set of zeros of a polynomial of degree at most  $d \geq 2$  in  $k$  variables with coefficients in an ordered domain  $D$  contained in a real closed field  $\mathbb{R}$ .*

- a) *There exists an algorithm for counting the number of  $s$ -a connected components of  $Z$  which uses  $d^{O(k\sqrt{k})}$  arithmetic operations in  $D$ .*

FIGURE 2. A roadmap of the torus in  $\mathbb{R}^3$ 

- b) *There exists an algorithm for deciding whether two given points, described by real univariate representations of degree at most  $d^{O(k)}$ , belong to the same  $s$ -a connected component of  $Z$  which uses  $d^{O(k\sqrt{k})}$  arithmetic operations in  $\mathbb{D}$ .*

*Remark 1.4.* We can always suppose without loss of generality that the zero set of a family of polynomials of degree at most  $d$  is defined by one single polynomial of degree at most  $2d$  by replacing the input polynomials by their sum of squares.

*Remark 1.5.* Even if the input is a polynomial with coefficients in the field of real numbers, the deformation techniques by infinitesimal elements we use make it necessary to perform computations on polynomials with coefficients in some non-archimedean real closed field. This is the reason why general real closed fields provide a natural framework for our work.

## 2. OUTLINE

We outline below the classical construction of a roadmap  $\text{RM}(\text{Zer}(Q, \mathbb{R}^k))$  for a bounded algebraic set  $\text{Zer}(Q, \mathbb{R}^k)$ , defined as the zero set of a polynomial  $Q$  contained in  $\mathbb{R}^k$ . The geometric ideas yielding this construction are due to Canny. The description below is similar to the one in [2, Chapter 15, Section 15.2].

A key ingredient of the algorithm is the construction of a particular finite set of points intersecting every  $s$ -a connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ . In the case of

a bounded and non-singular real algebraic set in  $\mathbb{R}^k$ , these points are nothing but the set of critical points of the projection to the  $X_1$ -coordinate on  $\text{Zer}(Q, \mathbb{R}^k)$ . In more general situations, the points we consider are called  $X_1$ -pseudo-critical points, since they are obtained as limits of the critical points of the projection to the  $X_1$ -coordinate of a bounded nonsingular algebraic hypersurface defined by a particular infinitesimal deformation of the polynomial  $Q$ . Their projections on the  $X_1$ -axis are called pseudo-critical values.

We first construct the “silhouette” which is the set of  $X_2$ -pseudo-critical points on  $\text{Zer}(Q, \mathbb{R}^k)$  along the  $X_1$ -axis by following continuously, as  $x$  varies on the  $X_1$ -axis, the  $X_2$ -pseudo-critical points on  $\text{Zer}(Q, \mathbb{R}^k)_x$ . Note that in case  $\text{Zer}(Q, \mathbb{R}^k)$  is a non-singular hypersurface, then the “silhouette” described above is the set of critical points of the projection map to the coordinates  $X_1$  and  $X_2$ . However, we are not assuming here that  $\text{Zer}(Q, \mathbb{R}^k)$  is a non-singular hypersurface. This results in curves and their endpoints on  $\text{Zer}(Q, \mathbb{R}^k)$ . The curves are continuous s-a curves parametrized by open intervals on the  $X_1$ -axis and their endpoints are points of  $\text{Zer}(Q, \mathbb{R}^k)$  above the corresponding endpoints of the open intervals. Since these curves and their endpoints include for every  $x \in \mathbb{R}$  the  $X_2$ -pseudo-critical points of  $\text{Zer}(Q, \mathbb{R}^k)_x$ , they meet every s-a connected component of  $\text{Zer}(Q, \mathbb{R}^k)_x$ . Thus, the set consisting of these curves and their endpoints, already satisfy  $\text{RM}_2$ . However, it is clear that this set might not be s-a connected in a s-a connected component and so  $\text{RM}_1$  might not be satisfied.

In order to ensure property  $\text{RM}_1$  we need to add more curves to the roadmap. For this purpose, we define the set of *distinguished values*  $\mathcal{D}$  as the union of the  $X_1$ -pseudo-critical values, and the first coordinates of the endpoints of the curves described in the previous paragraph. A *distinguished hyperplane* is a hyperplane defined by  $X_1 = v$ , where  $v$  is a distinguished value. The input points, the endpoints of the curves, and the intersections of the curves with the distinguished hyperplanes define the set of *distinguished points*,  $\mathcal{M}$ .

Let the distinguished values be  $v_1 < \dots < v_N$ . Note that amongst these are the  $X_1$ -pseudo-critical values. Above each interval  $(v_i, v_{i+1})$  we have constructed a collection of curves  $\mathcal{C}_i$  meeting every s-a connected component of  $\text{Zer}(Q, \mathbb{R}^k)_v$  for every  $v \in (v_i, v_{i+1})$ . Above each distinguished value  $v_i$  we have a set of distinguished points  $\mathcal{M}_i$ . Each curve in  $\mathcal{C}_i$  has an endpoint in  $\mathcal{M}_i$ , and another one in  $\mathcal{M}_{i+1}$ . Moreover, the union of the  $\mathcal{M}_i$  contains  $\mathcal{M}$ . We denote by  $\mathcal{C}$  the union of the  $\mathcal{C}_i$ .

The following key connectivity result is proved in [3, Lemma 15.9].

**Proposition 2.1.** *Let  $\mathcal{R} = \mathcal{C} \cup \text{Zer}(Q, \mathbb{R}^k)_{\mathcal{D}}$ . If  $P$  is a s-a connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ , then  $\mathcal{R} \cap P$  is s-a connected.*

Thus, in order to construct a roadmap of  $\text{Zer}(Q, \mathbb{R}^k)$  it suffices to repeat the same construction in each distinguished hyperplane  $H_i$  defined by  $X_1 = v_i$  with input  $Q(v_i, X_2, \dots, X_k)$  and the distinguished points in  $\mathcal{M}_{v_i}$  by making recursive calls to the algorithm. The following proposition is proved in [2, Proposition 15.7].

**Proposition 2.2.** *The s-a set  $\text{RM}(\text{Zer}(Q, \mathbb{R}^k), \mathcal{M})$  obtained by this construction is a roadmap for  $\text{Zer}(Q, \mathbb{R}^k)$  containing  $\mathcal{M}$ .*

To summarize, classical roadmap algorithms based on Canny’s construction proceed by first considering the “silhouette”, consisting of curves in the  $X_1$ -direction,

and then making recursive calls to the same algorithm at certain hyperplane sections of  $\text{Zer}(Q, \mathbb{R}^k)$ , so that the dimension of the ambient space drops by 1 at each recursive call.

The main difference between classical roadmap algorithms and the algorithms described in [8] and in the current paper is that instead of considering curves in the  $X_1$ -direction and making recursive calls to the same algorithm at certain hyperplane sections of  $\text{Zer}(Q, \mathbb{R}^k)$  corresponding to special values of  $X_1$ , so that the dimension of the ambient space drops by 1, we consider a  $p$ -dimensional subset  $W^{(p)}$  of  $\text{Zer}(Q, \mathbb{R}^k)$  where  $1 \leq p \leq k$ , and make recursive calls at certain  $(k - p)$ -dimensional fibers of  $\text{Zer}(Q, \mathbb{R}^k)$ , so that the dimension of the ambient space drops by  $p$ .

The main topological result, analogous to Proposition 2.1, is that if the set  $\text{Zer}(Q, \mathbb{R}^k)$  satisfies certain conditions, such as having only isolated singular points, then the s-a set which is the union of  $W$  and these fibers are s-a connected. This is proved in Section 3. It follows, though not immediately, that for a general real algebraic set,  $\text{Zer}(Q, \mathbb{R}^k)$ , in order to produce a roadmap of  $\text{Zer}(Q, \mathbb{R}^k)$  it suffices to compute:

- (1) a roadmap of a certain s-a subset  $W$  of an infinitesimal deformation of  $\text{Zer}(Q, \mathbb{R}^k)$  passing through a carefully chosen set of points, and taking the limit of the curves so obtained by letting the perturbation variable go to 0;
- (2) roadmaps of certain fibers in a  $(k - p)$ -dimensional ambient space, using recursive calls.

The fact that in the new algorithm we are fixing a whole block of  $p$  variables at a time necessitates introducing a new kind of algebraic representation which we call “real block representation”. This notion is defined in Section 4, where we also explain how to represent curves over such blocks.

In Section 5, we consider the case when  $W$  is low-dimensional and described by equations having a special structure. Adapting an algorithm from [2, Algorithm 15.3] we show how to compute a roadmap of  $W$  in this case with complexity depending in a crucial way on the dimension of  $W$ . The general case, requiring the use of a deformation technique and a limit process, is described in Section 6.

Finally, we obtain in Section 7 a baby step - giant step roadmap algorithm for a general algebraic set. We prove its correctness, as well as the improved complexity bound.

The algorithm for computing efficiently limits of curve segments is quite technical. Since this technicality can obscure the ideas behind the main algorithm, for the sake of readability we have postponed the details behind taking limits of curves to a separate section (Section 8).

Throughout the paper, we use as a basic reference [2]. We cite [3] instead when the precise statements needed are not included in [2].

### 3. CONNECTIVITY RESULTS

In this section we prove a topological result about connectivity which will be used in proving the correctness of our algorithm later. The statement of the result, as well as the main ideas of the proof, is influenced by [8, Theorem 14]. It is a direct generalization of Proposition 2.1 to the case of projection onto more than one variable.

We denote by  $\mathbb{R}$  a real closed field.

**Notation 3.1.** For  $1 \leq p < k$ , we denote by  $\pi_p$  the projection

$$(x_1, \dots, x_k) \mapsto x_p.$$

For  $1 \leq q \leq p < k$ , we denote by  $\pi_{[q,p]} : \mathbb{R}^k \rightarrow \mathbb{R}^{p-q+1}$  the projection

$$(x_1, \dots, x_k) \mapsto (x_q, \dots, x_p).$$

For any pair of s-a subsets  $S \subset \mathbb{R}^k$ , and  $T \subset \mathbb{R}^p$ , we denote by  $S_T$  the s-a set  $\pi_{[1,p]}^{-1}(T) \cap S$ , and  $S_y$  rather than  $S_{\{y\}}$ , for  $y \in \mathbb{R}^p$ . We also write  $S_{<a}$  and  $S_{\leq a}$  rather than  $S_{(-\infty, a)}$  and  $S_{(-\infty, a]}$ , for  $a \in \mathbb{R}$ .

We denote as before by  $\text{Zer}(Q, \mathbb{R}^k)$  the algebraic set of zeros of a polynomial  $Q \in \mathbb{R}[X_1, \dots, X_k]$  contained in  $\mathbb{R}^k$ . Note that for a non-constant polynomial  $Q$ , the real dimension of  $\text{Zer}(Q, \mathbb{R}^k)$  is not necessarily equal to  $k - 1$ , and indeed  $\text{Zer}(Q, \mathbb{R}^k)$  might even be empty. In fact, over any real closed field, algebraic sets defined by one equation coincide with general algebraic sets since replacing several equations by their sum of squares does not modify the zero set. A  **$Q$ -singular point** is a point  $x \in \mathbb{R}^k$  such that

$$Q(x) = \frac{\partial Q}{\partial X_1}(x) = \dots = \frac{\partial Q}{\partial X_k}(x) = 0.$$

Note that this is an algebraic property related to the polynomial  $Q$  rather than a geometric property of the underlying set  $\text{Zer}(Q, \mathbb{R}^k)$ : two equations can define the same algebraic set but have different sets of singular points.

Similarly a  **$Q$ -critical point** of  $\pi_1$  is a point  $x \in \mathbb{R}^k$  such that

$$Q(x) = \frac{\partial Q}{\partial X_2}(x) = \dots = \frac{\partial Q}{\partial X_k}(x) = 0.$$

To simplify notation, when there will be no ambiguity regarding  $Q$ , we will simply refer to singular/critical points.

In this paper, we will be using constantly the notion of s-a connected components of a s-a set [2, Section 5.2]. Note that, in particular, a s-a connected component is always non-empty by definition (see [3, Theorem 5.21] and the definition of s-a connected components following it). In particular, the empty set has no s-a connected component.

**Property 3.2.** We now consider for  $1 \leq p < k$  a tuple

$$(V, \mathcal{M}, W^{(p)}, \mathcal{M}^{(p)}, \mathcal{D}^{(p)})$$

with the following properties:

- (1)  $V \subset \mathbb{R}^k$  is the union of certain bounded s-a connected components of an algebraic set  $\text{Zer}(Q, \mathbb{R}^k) \subset \mathbb{R}^k$ , such that the  $Q$ -critical points of the map  $\pi_1$  on  $V$  (which contains in particular the  $Q$ -singular points contained in  $V$ ) form the finite set  $\mathcal{M} \subset V$ ;
- (2)  $W^{(p)} \subset V$  is a closed s-a set of dimension  $p$ , such that for each  $y \in \mathbb{R}^p$ ,  $W_y^{(p)}$  (cf. Notation 3.1) is a finite set of points having non-empty intersection with every s-a connected component of  $V_y$ ;
- (3)  $\mathcal{M}^{(p)} \subset V$  is a finite subset such that the intersection of  $\mathcal{M}^{(p)}$  with every s-a connected component of  $W_a^{(p)}$  is non-empty, for  $a \in \mathcal{D}^{(p)} = \pi_1(\mathcal{M}^{(p)})$ . Moreover, for every interval  $[a, b]$  and  $c \in [a, b]$  with  $\{c\} \supset \mathcal{D}^{(p)} \cap [a, b]$ ,



if  $C$  is a  $s$ -a connected component of  $W_{[a,b]}^{(p)}$ , then  $C_c$  is a  $s$ -a connected component of  $W_c^{(p)}$ .

A tuple

$$(V, \mathcal{M}, W^{(p)}, \mathcal{M}^{(p)}, \mathcal{D}^{(p)})$$

is said to satisfy Property 3.2 if it satisfies the above properties (1) to (3).

Now we state the main result of this section. It generalizes Proposition 2.1 as well as [8, Theorem 14], in the special case when Property 3.2 holds.

**Proposition 3.3.** *Let*

$$(V, \mathcal{M}, W^{(p)}, \mathcal{M}^{(p)}, \mathcal{D}^{(p)})$$

*satisfy Property 3.2,*

$$\mathcal{N} = \pi_{[1,p]}(\mathcal{M}), \mathcal{N}^{(p)} = \pi_{[1,p]}(\mathcal{M}^{(p)}),$$

*and*

$$\mathcal{S} = W^{(p)} \cup V_{\mathcal{N} \cup \mathcal{N}^{(p)}}.$$

*For every  $s$ -a connected component  $C$  of  $V$ ,  $C \cap \mathcal{S}$  is non-empty and  $s$ -a connected.*

*Remark 3.4.* In order to understand the situation, the following example of a tuple satisfying Property 3.2 can be useful:

- (1) the torus  $V \subset \mathbb{R}^3$  defined as the set of zeros of the equation

$$Q = 36(X_1^2 + \left(\frac{12X_2 + 5X_3}{13}\right)^2) - (X_1^2 + X_2^2 + X_3^2 + 8)^2,$$

([4], page 40, figure 2.5),  $p = 1$ , the four critical points  $\mathcal{M} \subset V$  of the map  $\pi_1$  restricted to  $V$ ;

- (2) the silhouette  $W^{(1)} \subset V$  defined by

$$Q = \frac{\partial Q}{\partial X_3} = 0;$$

- (3) the six critical values  $\mathcal{D}^{(1)} \subset \mathbb{R}$  of the map  $\pi_1$  restricted to the silhouette  $W$ , and the intersection  $\mathcal{M}^{(1)}$  of the corresponding six fibers with the silhouette  $W^{(1)}$ .

The tuple

$$(V, \mathcal{M}, W^{(1)}, \mathcal{M}^{(1)}, \mathcal{D}^{(1)})$$

satisfies Property 3.2.

Finally,  $\mathcal{S}$  is the union of the silhouette and the intersection of the torus with the six curves which are the fibers of  $V$  at the distinguished values  $\mathcal{D}^{(1)}$ .

The rest of this section is devoted to prove Proposition 3.3. We need preliminaries about non-archimedean extensions of the base real closed field  $\mathbb{R}$ .

*Remark 3.5.* A typical non-archimedean extension of  $\mathbb{R}$  is the field  $\mathbb{R}\langle\varepsilon\rangle$  of algebraic Puiseux series with coefficients in  $\mathbb{R}$ , which coincide with the germs of  $s$ -a continuous functions (see [2, Chapter 2, Section 6 and Chapter 3, Section 3]). An element  $x \in \mathbb{R}\langle\varepsilon\rangle$  is bounded over  $\mathbb{R}$  if  $|x| \leq r$  for some  $0 \leq r \in \mathbb{R}$ . The subring  $\mathbb{R}\langle\varepsilon\rangle_b$  of elements of  $\mathbb{R}\langle\varepsilon\rangle$  bounded over  $\mathbb{R}$  consists of the Puiseux series with non-negative

exponents. We denote by  $\lim_\varepsilon$  the ring homomorphism from  $R\langle\varepsilon\rangle_b$  to  $R$  which maps  $\sum_{i \in \mathbb{N}} a_i \varepsilon^{i/q}$  to  $a_0$ . So, the mapping  $\lim_\varepsilon$  simply replaces  $\varepsilon$  by 0 in a bounded Puiseux series. Given  $S \subset R\langle\varepsilon\rangle^k$ , we denote by  $\lim_\varepsilon(S) \subset R^k$  the image by  $\lim_\varepsilon$  of the elements of  $S$  whose coordinates are bounded over  $R$ .

More generally, let  $R'$  be a real closed field extension of  $R$ . If  $S \subset R^k$  is a s-a set, defined by a boolean formula  $\Phi$  with coefficients in  $R$ , we denote by  $\text{Ext}(S, R')$  the extension of  $S$  to  $R'$ , i.e. the s-a subset of  $R'^k$  defined by  $\Phi$ . The first property of  $\text{Ext}(S, R')$  is that it is well defined, i.e. independent of the formula  $\Phi$  describing  $S$  [2, Proposition 2.87]. Many properties of  $S$  can be transferred to  $\text{Ext}(S, R')$ : for example  $S$  is non-empty if and only if  $\text{Ext}(S, R')$  is non-empty; also  $S$  is s-a connected if and only if  $\text{Ext}(S, R')$  is s-a connected [2, Proposition 5.24].

Moreover, if Property 3.2 (2) holds for  $V, W$ , i.e. for every  $y \in R^p$ ,  $W_y$  is a finite set of points having non-empty intersection with every s-a connected component of  $V_y$ , then Property 3.2 (2) holds for  $\text{Ext}(V, R'), \text{Ext}(W, R')$ , i.e. for each  $y' \in R'^p$ ,  $\text{Ext}(W, R')_{y'}$  is a finite set of points having non-empty intersection with every s-a connected component of  $\text{Ext}(V, R')_{y'}$ . Indeed, by Hardt's s-a triviality theorem [2, Theorem 5.45], one can find a finite partition of  $R^p$  into s-a sets  $T_i$ ,  $i = 1, \dots, r$ , a finite partition of  $V_{T_i}$  into s-a sets  $S_{i,j}$  and an integer  $n_i > 0$  such that  $S_{i,j}$  is s-a homeomorphic to  $T_i \times (S_{i,j})_{y_i}$  for some  $y_i \in T_i$ , and for all  $y \in T_i$ , the s-a connected components of  $V_y$  are  $(S_{i,j})_y$  and  $W_y$  has  $n_i$  points. By Tarski-Seidenberg's transfer principle [2, Theorem 2.80],  $\text{Ext}(S_{i,j}, R')$  is s-a homeomorphic to  $\text{Ext}(T_i, R') \times \text{Ext}(S_{i,j}, R')_{y_i}$ , and for all  $y' \in R'^p$ , there exists  $i$  such that  $y' \in \text{Ext}(T_i, R')$ , the sets  $\text{Ext}(S_{i,j}, R')_{y'}$  are the s-a connected components of  $\text{Ext}(V, R')_{y'}$  and the intersection of  $\text{Ext}(W, R')_{y'}$  and  $\text{Ext}(S_{i,j}, R')_{y'}$  has exactly  $n_i$  points.

Let  $V$  be the union of a subset of the bounded s-a connected components of an algebraic set  $\text{Zer}(Q, R^k) \subset R^k$ . Suppose also that the set  $\mathcal{M}$  of points which are singular points of  $\text{Zer}(Q, R^k)$  or critical points of  $\pi_1$  on  $\text{Zer}(Q, R^k)$  and which belong to  $V$  is finite. We now prove two preliminary results (Lemma 3.6 and Lemma 3.7 below) about the pair  $(V, \mathcal{M})$  which will be needed in the proof of Proposition 3.3.

In this paper a *s-a path* is a s-a continuous function  $\gamma$  from a closed interval  $[a, b] \subset R$  to  $R^k$ . Note that a s-a set is s-a connected if and only if it is s-a path connected [2, Theorem 5.23].

**Lemma 3.6.** *Let  $C$  be a s-a connected component of  $V_{\leq b}$  such that  $C \cap V_b$  is not empty.*

- (1) *If  $\dim(C) = 0$ ,  $C$  is a point contained in  $\mathcal{M}$ .*
- (2) *If  $\dim(C) \neq 0$ ,  $C_{<b}$  is non-empty. Let  $B_1, \dots, B_s$  be the s-a connected components of  $C_{<b}$ . Then,*
  - (a) *for each  $i$ ,  $1 \leq i \leq s$ ,  $\overline{B_i} \cap \mathcal{M} \neq \emptyset$ ;*
  - (b) *if there exist  $i, j$ ,  $1 \leq i < j \leq s$  such that  $\overline{B_i} \cap \overline{B_j} \neq \emptyset$ , then  $\overline{B_i} \cap \overline{B_j} \subset \mathcal{M}$ ;*
  - (c)  *$\cup_{i=1}^s \overline{B_i} = C$ , and hence  $\cup_{i=1}^s \overline{B_i}$  is s-a connected.*

*Proof.* Part 1 follows immediately from [3, Proposition 7.3]. We prove Part 2. Since  $\mathcal{M}$  is finite, there is a non-singular point  $x \in C_b$  which is non-critical for  $\pi_1$  on  $V$ . Let  $T_x V$  denote the tangent space to  $V$  at  $x$ . So  $T_x V$  is not orthogonal to the  $X_1$  axis, and the s-a implicit function theorem [2, Theorem 3.25] implies that  $C_{<b}$  is non-empty.

Part 2) a) and 2 b) are immediate consequences of Proposition 7.3 in [3].

We prove 2) c). Clearly,  $\cup_{i=1}^s \overline{B_i} \subset C$ . Moreover since  $C_{<b}$  is non-empty,  $\cup_{i=1}^s \overline{B_i}$  is also non-empty. Suppose that  $x \in A = C \setminus \cup_{i=1}^s \overline{B_i}$ . For  $r > 0$  sufficiently small,  $\mathcal{B}_k(x, r) \cap C_{<b} = \emptyset$  (where  $\mathcal{B}_k(x, r)$  is the  $k$ -dimensional open ball of center  $x$  and radius  $r$ ). Note that  $\pi_1(x) = b$ , since otherwise  $x$  belongs to  $C_{<b}$ , and thus to one of the  $B_i$ 's.

Applying [3, Proposition 7.3], we deduce from the fact that  $\mathcal{B}_k(x, r) \cap C_{<b} = \emptyset$  that  $x$  is either a  $Q$ -singular point, or a  $Q$ -critical point of  $\pi_1$  on  $V$ . In other words  $x \in \mathcal{M}$ . But since by assumption  $\mathcal{M}$  is finite, this implies that  $A$  is a finite set and is closed. Since  $C$  is s-a connected, and  $\cup_{i=1}^s \overline{B_i}$  closed and non-empty,  $A$  must be empty.  $\square$

**Lemma 3.7.** *Suppose that  $b \notin \pi_1(\mathcal{M})$ . Let  $C$  be a s-a connected component of  $V_{\leq b}$ . If  $a < b$  and  $(a, b] \cap \pi_1(\mathcal{M})$  is empty, then  $C_{\leq a}$  is a s-a connected component of  $V_{\leq a}$ .*

*Proof.* We first prove that  $C_{\leq a}$  is non-empty. Since  $C$  is non-empty because it is a s-a connected component of  $V_{\leq b}$ , there must exist  $a' \in \mathbb{R}$ , with  $a' \leq b$ , such that  $C_{\leq a'}$  is non-empty, but  $C_{\leq a''}$  is empty for all  $a'' < a'$ . In this case, using Lemma 3.6,  $a' \in \pi_1(\mathcal{M})$ , since  $(a, b] \cap \pi_1(\mathcal{M})$  is empty,  $a' \leq a$  and  $C_{\leq a}$  is non-empty.

We now show that  $C_{\leq a}$  is s-a connected. This together with the fact shown above implies that  $C_{\leq a}$  is a s-a connected component of  $V_{\leq a}$ . Let  $x$  and  $y$  be two points of  $C_{\leq a}$  and  $\gamma : [0, 1] \rightarrow C$  be a s-a path connecting  $x$  to  $y$  inside  $C$ . We want to prove that there is a s-a path connecting  $x$  to  $y$  inside  $C_{\leq a}$ .

If  $\text{Im}(\gamma) \subset C_{\leq a}$ , there is nothing to prove.

If  $\text{Im}(\gamma) \not\subset C_{\leq a}$ , then there exists  $c \in \mathbb{R}$  such that for all  $d \in \mathbb{R}$  such that  $a < d < c$ ,  $\text{Im}(\gamma) \cap \text{Zer}(Q)_d \neq \emptyset$ .

Let  $\varepsilon$  be a positive infinitesimal. Then

$$\text{Ext}(\gamma([0, 1]), \mathbb{R}\langle\varepsilon\rangle) \cap \text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{a+\varepsilon} \neq \emptyset$$

using [2, Proposition 3.17]. Since

$$\{u \in [0, 1] \subset \mathbb{R}\langle\varepsilon\rangle \mid \text{Ext}(\gamma, \mathbb{R}\langle\varepsilon\rangle)(u) \in \text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{<a+\varepsilon}\}$$

and

$$\{u \in [0, 1] \subset \mathbb{R}\langle\varepsilon\rangle \mid \text{Ext}(\gamma, \mathbb{R}\langle\varepsilon\rangle)(u) \in \text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{[a+\varepsilon, b]}\}$$

are s-a subsets of  $[0, 1] \subset \mathbb{R}\langle\varepsilon\rangle$ , there exists by [2, Corollary 2.79] a finite partition  $\mathfrak{P}$  of  $[0, 1] \subset \mathbb{R}\langle\varepsilon\rangle$  such that for each open interval  $(u, v)$  of  $\mathfrak{P}$ ,  $\text{Ext}(\gamma, \mathbb{R}\langle\varepsilon\rangle)(u, v)$  is either contained in the set  $\text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{<a+\varepsilon}$ , or in the set  $\text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{[a+\varepsilon, b]}$ , with  $\gamma(u)$  and  $\gamma(v)$  in  $\text{Ext}(C, \mathbb{R}\langle\varepsilon\rangle)_{a+\varepsilon}$ .

If  $\text{Ext}(\gamma, \mathbb{R}\langle\varepsilon\rangle)(u, v)$  is contained in  $\text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{[a+\varepsilon, b]}$ , we can replace  $\gamma$  by a s-a path  $\gamma'_{[u, v]}$  connecting  $\gamma(u)$  to  $\gamma(v)$  inside  $\text{Ext}(C, \mathbb{R}\langle\varepsilon\rangle)_{a+\varepsilon}$ . Note that there is no  $Q$ -critical point of  $\pi_1$  in  $\text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle)_{[a+\varepsilon, b]}$  and  $\text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle)_{[a+\varepsilon, b]}$  contains no  $Q$ -singular point by [2, Proposition 3.17] while  $\text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle) \subset \text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)$  by [2, Proposition 2.87].

By [3, Proposition 15.1 b], if  $C'$  is a s-a connected component of  $\text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle)_{[a+\varepsilon, b]}$ ,  $C'_{a+\varepsilon}$  is a s-a connected component of  $\text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle)_{a+\varepsilon}$ .

Construct a s-a path  $\gamma'$  from  $x$  to  $x'$  inside  $\text{Ext}(C, \mathbb{R}\langle\varepsilon\rangle)_{\leq a+\varepsilon}$ , obtained by concatenating pieces of  $\gamma$  inside  $\text{Zer}(Q, \mathbb{R}\langle\varepsilon\rangle^k)_{<a+\varepsilon}$  and the paths  $\gamma'_{(u, v)}$  connecting  $\gamma(u)$  to  $\gamma(v)$  for  $(u, v)$  such that

$$\text{Ext}(\gamma, \mathbb{R}\langle\varepsilon\rangle)(u, v) \subset \text{Ext}(V, \mathbb{R}\langle\varepsilon\rangle)_{[a+\varepsilon, b]}.$$

Note that such a s-a connected path  $\gamma'$  is closed and bounded. Applying [2, Proposition 12.43],  $\lim_{\varepsilon}(\gamma'([0, 1]))$  is s-a connected, contains  $x$  and  $x'$  and is contained in  $\lim_{\varepsilon}(\text{Ext}(C, R(\varepsilon))_{\leq a+\varepsilon}) = C_{\leq a}$ . This proves the lemma.  $\square$

**Notation 3.8.** If  $S \subset \mathbb{R}^k$  is s-a set and  $x \in S$ , then we denote by  $\mathcal{C}(S, x)$  the s-a connected component of  $S$  containing  $x$ .

We are now ready to prove Proposition 3.3.

*Proof of Proposition 3.3.* For every  $a \in \mathbb{R}$ , we say that property  $\mathbf{P}(a)$  holds if: for any s-a connected component  $C$  of  $V_{\leq a}$ ,  $C \cap \mathcal{S}$  is s-a connected.

We prove that for all  $a$  in  $\mathbb{R}$ , the property  $\mathbf{P}(a)$  holds. Since  $V$  is bounded, the proposition follows from the property  $\mathbf{P}(a)$  for any  $a \geq \max_{x \in V} \pi_1(x)$ .

Let  $\mathcal{D} = \pi_1(\mathcal{M} \cup \mathcal{M}^{(p)})$ .

The proof uses two intermediate results:

**Step 1:** For every  $a \in \mathcal{D}$ , property  $\mathbf{P}(a)$  implies property  $\mathbf{P}(b)$  if  $b \in \mathbb{R}$  with  $(a, b] \cap \mathcal{D} = \emptyset$ .

**Step 2:** For every  $b \in \mathcal{D}$ , if property  $\mathbf{P}(a)$  holds for all  $a < b$ , then property  $\mathbf{P}(b)$  holds.

Since for  $a < \min_{x \in V} \pi_1(x)$ , the property  $\mathbf{P}(a)$  holds vacuously, and the combination of these two results gives by an easy induction the property  $\mathbf{P}(a)$  for all  $a$  in  $\mathbb{R}$ .

We now prove the two steps.

**Step 1.** We suppose that  $a \in \mathcal{D}$ , and that the property  $\mathbf{P}(a)$  holds. Take  $b \in \mathbb{R}$ ,  $a < b$  with  $(a, b] \cap \mathcal{D} = \emptyset$  and prove that the property  $\mathbf{P}(b)$  holds. Let  $C$  be a s-a connected component of  $V_{\leq b}$ . We have to prove that  $C \cap \mathcal{S}$  is non-empty and s-a connected.

Since  $(a, b] \cap \mathcal{D} = \emptyset$ , it follows that  $\mathcal{M}_{(a, b]} = \emptyset$ , and  $C_{\leq a}$  is a s-a connected component of  $V_{\leq a}$  using Lemma 3.7. So, using property  $\mathbf{P}(a)$ , we see that  $C_{\leq a} \cap \mathcal{S}$  is non-empty and s-a connected.

If  $C_{\leq a} \cap \mathcal{S} = C \cap \mathcal{S}$ , there is nothing to prove. Otherwise, let  $x \in C \cap \mathcal{S}$  such that  $x \notin C_{\leq a}$ . We prove that  $x$  can be s-a connected to a point in  $C_{\leq a} \cap \mathcal{S}$  by a s-a path in  $C \cap \mathcal{S}$ , which is enough to prove that  $C \cap \mathcal{S}$  is s-a connected.

Since  $\pi_1(x) \in (a, b]$  and  $(a, b] \cap \mathcal{D} = \emptyset$ , we deduce that  $\pi_1(x) \notin \mathcal{D}$  and  $x \notin V_{\mathcal{N} \cup \mathcal{N}^{(p)}}$ . So, from  $x \in \mathcal{S}$ , we get  $x \in W^{(p)}$ . We note that  $\mathcal{C}(W_{[a, b]}^{(p)}, x) \subset C$ . By Property 3.2 (3) applied to  $\mathcal{C}(W_{[a, b]}^{(p)}, x)$  (noting that  $(a, b] \cap \mathcal{D}_2 \subset (a, b] \cap \mathcal{D} = \emptyset$ ) we have that  $a \in \pi_1(\mathcal{C}(W_{[a, b]}^{(p)}, x))$  and  $\mathcal{C}(W_{[a, b]}^{(p)}, x)_a$  is non-empty. Hence there exists a s-a path connecting  $x$  to a point in  $\mathcal{C}(W_{[a, b]}^{(p)}, x)_a$  inside  $\mathcal{C}(W_{[a, b]}^{(p)}, x)$ . Since  $\mathcal{C}(W_{[a, b]}^{(p)}, x) \subset W^{(p)} \subset \mathcal{S}$  and  $\mathcal{C}(W_{[a, b]}^{(p)}, x) \subset C$ , it follows that  $\mathcal{C}(W_{[a, b]}^{(p)}, x) \subset C \cap \mathcal{S}$  and we are done.

**Step 2.** We suppose that  $b \in \mathcal{D}$ , and that the property  $\mathbf{P}(a)$  holds for all  $a < b$ . We prove that the property  $\mathbf{P}(b)$  holds.

Let  $C$  be a s-a connected component of  $V_{\leq b}$ . If  $C_b = \emptyset$ , there is nothing to prove. Suppose that  $C_b$  is non-empty; we have to prove that  $C \cap \mathcal{S}$  is s-a connected.

If  $\dim(C) = 0$ ,  $C$  is a point, belonging to  $\mathcal{M} \subset \mathcal{S}$  by Lemma 3.6. So  $C \cap \mathcal{S}$  is s-a connected.

Hence, we can assume that  $\dim(C) > 0$ , so that  $C_{< b}$  is non-empty by Lemma 3.6.

Our aim is to prove that  $C \cap \mathcal{S}$  is s-a connected. We do this in two steps. We prove the following statements:

- (a) If  $B$  is a s-a connected component of  $C_{<b}$ , then  $\overline{B} \cap \mathcal{S}$  is s-a connected, and, using (a),
- (b)  $C \cap \mathcal{S}$  is non-empty and s-a connected.

**Proof of (a)** We prove that if  $B$  is a s-a connected component of  $C_{<b}$ , then  $\overline{B} \cap \mathcal{S}$  is s-a connected.

Since  $\overline{B}$  contains a point of  $\mathcal{M}$  it follows that  $\overline{B} \cap \mathcal{S}$  is not empty.

Note that if  $\overline{B} \cap \mathcal{S} = B \cap \mathcal{S}$ , then there exists  $a$  with

$$\max(\{\pi_1(x) \mid x \in B \cap \mathcal{S}\}) < a < b,$$

with  $B \cap \mathcal{S} = (B \cap \mathcal{S})_{\leq a}$  and  $B_{\leq a}$  s-a connected using Lemma 3.7. So  $B \cap \mathcal{S}$  is s-a connected since the property **P**( $a$ ) holds.

We now suppose that  $(\overline{B} \setminus B) \cap \mathcal{S}$  is non-empty. Taking  $x \in (\overline{B} \setminus B) \cap \mathcal{S}$ , we are going to show that  $x$  can be connected to a point  $z$  in  $B \cap \mathcal{S}$  by a s-a path  $\gamma$  inside  $\overline{B} \cap \mathcal{S}$ . Notice that  $\pi_1(x) = b$ .

We first prove that we can assume without loss of generality that  $x \in W^{(p)}$ . Otherwise, since  $x \in \mathcal{S}$  and  $\mathcal{S} = W^{(p)} \cup V_{\mathcal{N} \cup \mathcal{N}^{(p)}}$ , we must have that  $x \in V_y$  with  $y = \pi_{[1,p]}(x)$ , and  $V_y \subset \mathcal{S}$ . Let  $A = \mathcal{C}(V_y \cap \overline{B}, x)$ . We now prove that  $A \cap W_y^{(p)} \neq \emptyset$ . Using the Curve Selection Lemma [4, Theorem 2.5.5] choose a s-a path  $\gamma : [0, \varepsilon] \rightarrow \text{Ext}(\overline{B}, \mathcal{R}(\varepsilon))$  such that  $\gamma(0) = x$ ,  $\lim_{\varepsilon} \gamma(\varepsilon) = x$  and  $\gamma((0, \varepsilon]) \subset \text{Ext}(B, \mathcal{R}(\varepsilon))$ . Let  $y_\varepsilon = \pi_{[1,p]}(\gamma(\varepsilon))$  and

$$A(\varepsilon) = \mathcal{C}(\text{Ext}(B, \mathcal{R}(\varepsilon))_{y(\varepsilon)}, \gamma(\varepsilon)).$$

Note that  $x \in \lim_{\varepsilon} A(\varepsilon) \subset A$ .

By Remark 3.5,  $\text{Ext}(B, \mathcal{R}(\varepsilon))$  is a s-a connected component of  $\text{Ext}(V_{<b}, \mathcal{R}(\varepsilon))$  which implies that  $A(\varepsilon)$  is a s-a connected component of  $\text{Ext}(V, \mathcal{R}(\varepsilon))_{y(\varepsilon)}$ . By Property 3.2 (2) and Remark 3.5,  $\text{Ext}(W^{(p)}, \mathcal{R}(\varepsilon))_{y(\varepsilon)} \cap A(\varepsilon) \neq \emptyset$ . Then, since  $\text{Ext}(W^{(p)}, \mathcal{R}(\varepsilon))_{y(\varepsilon)} \cap A(\varepsilon)$  is bounded over  $\mathcal{R}$ , we deduce that

$$\lim_{\varepsilon} (\text{Ext}(W^{(p)}, \mathcal{R}(\varepsilon))_{y(\varepsilon)} \cap A(\varepsilon))$$

is a non-empty subset of  $W_y^{(p)} \cap A$ .

Now connect  $x$  to a point  $x' \in W_y^{(p)}$  by a s-a path whose image is contained in  $A \subset \overline{B}_y \subset (\overline{B} \setminus B) \cap \mathcal{S}$ . Thus, replacing  $x$  by  $x'$  if necessary we can assume that  $x \in W^{(p)}$  as claimed.

There are four cases, namely

- (1)  $x \in \mathcal{M} \cup \mathcal{M}^{(p)}$ ;
- (2)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$  and  $\mathcal{C}(W_b^{(p)}, x) \not\subset \overline{B}$ ;
- (3)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$ ,  $\mathcal{C}(W_b^{(p)}, x) \subset \overline{B}$  and  $b \in \mathcal{D}^{(p)}$ ;
- (4)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$ ,  $\mathcal{C}(W_b^{(p)}, x) \subset \overline{B}$  and  $b \notin \mathcal{D}^{(p)}$ ;

that we consider now.

- (1)  $x \in \mathcal{M} \cup \mathcal{M}^{(p)}$ :

Define  $y = \pi_{[1,p]}(x) \in \mathcal{R}^p$ , and note that  $V_y \subset \mathcal{S}$ . Since  $x \in \overline{B}$ , and  $B$  is bounded,  $y \in \pi_{[1,p]}(\overline{B}) = \overline{\pi_{[1,p]}(B)}$ . Now let  $\varepsilon > 0$  be an infinitesimal. By applying the Curve Selection Lemma [4, Theorem 2.5.5] to the set  $B$  and  $x \in \overline{B}$ , and then projecting to  $\mathcal{R}^p$  using  $\pi_{[1,p]}$  we obtain that there

exists  $y(\varepsilon) \in R\langle\varepsilon\rangle^p$  infinitesimally close to  $y$  with  $\pi_1(y(\varepsilon)) < \pi_1(y) = b$ , and  $x \in \lim_\varepsilon \text{Ext}(V, R\langle\varepsilon\rangle)_{y(\varepsilon)}$ . Let  $x(\varepsilon) \in \text{Ext}(V, R\langle\varepsilon\rangle)_{y(\varepsilon)}$  be such that  $\lim x(\varepsilon) = x$ . Moreover, by Property 3.2 (2) and Remark 3.5 we have that  $\text{Ext}(W^{(p)}, R\langle\varepsilon\rangle)_{y(\varepsilon)}$  is non-empty and meets every s-a connected component of  $\text{Ext}(V, R\langle\varepsilon\rangle)_{y(\varepsilon)}$ . Note that

$$\text{Ext}(V, R\langle\varepsilon\rangle)_{y(\varepsilon)} = \text{Ext}(V_{\leq b}, R\langle\varepsilon\rangle)_{y(\varepsilon)} = \text{Ext}(V_{< b}, R\langle\varepsilon\rangle)_{y(\varepsilon)}.$$

Let

$$x'(\varepsilon) \in \text{Ext}(W^{(p)}, R\langle\varepsilon\rangle)_{y(\varepsilon)} \cap \mathcal{C}(\text{Ext}(B, R\langle\varepsilon\rangle)_{y(\varepsilon)}, x(\varepsilon)),$$

and  $x' = \lim_\varepsilon x'(\varepsilon)$ . Since  $\lim_\varepsilon x(\varepsilon) = x$  and  $\lim_\varepsilon \mathcal{C}(\text{Ext}(B, R\langle\varepsilon\rangle)_{y(\varepsilon)}, x(\varepsilon))$  is s-a connected,

$$\lim_\varepsilon \mathcal{C}(\text{Ext}(B, R\langle\varepsilon\rangle)_{y(\varepsilon)}, x(\varepsilon)) \subset \mathcal{C}(\overline{B}_y, x).$$

Now choose a s-a path  $\gamma_1$  connecting  $x$  to  $x'$  inside  $\mathcal{C}(\overline{B}_y, x)$  (and hence inside  $\mathcal{S}$  since  $\mathcal{C}(\overline{B}_y, x) \subset V_y \subset \mathcal{S}$ ). Since  $x'(\varepsilon)$  has coordinates which are algebraic Puiseux series in  $\varepsilon$ , there exists a positive element  $t_0 \in \mathbb{R}$ , and a s-a curve  $\gamma_2 : [0, t_0] \rightarrow \mathbb{R}^k$  defined over  $\mathbb{R}$ , such that  $x' = \gamma_2(0)$ , and  $x'(\varepsilon) \in \text{Ext}(\gamma_2, R\langle\varepsilon\rangle)(\varepsilon)$  (see [2, Theorem 3.14]).

The concatenation of  $\text{Ext}(\gamma_1, R\langle\varepsilon\rangle), \text{Ext}(\gamma_2, R\langle\varepsilon\rangle)|_{[0, \varepsilon]}$  gives a s-a path  $\gamma$  having the required property, after replacing  $\varepsilon$  by a sufficiently small positive element of  $\mathbb{R}$ .

- (2)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$  and  $\mathcal{C}(W_b^{(p)}, x) \not\subset \overline{B}$ :

There exists  $x' \in \mathcal{C}(W_b^{(p)}, x)$ ,  $x' \notin \overline{B}$  and a s-a path  $\gamma : [0, 1] \rightarrow \mathcal{C}(W_b^{(p)}, x)$ , with  $\gamma(0) = x, \gamma(1) = x'$ . Since  $x' \notin \overline{B}$ , it follows that for  $t_1 = \max\{0 \leq t < 1 \mid \gamma(t) \in \overline{B}\}$ ,  $\gamma(t_1) \in \mathcal{M}$ . To see this observe that by Lemma 3.6 (2c), it follows that  $\gamma(t_1) \in \overline{B} \cap \overline{B'}$ , where  $B'$  is a s-a connected component of  $C_{< b}$  distinct from  $B$ . It then follows from Lemma 3.6 (2b) that  $\gamma(t_1) \in \mathcal{M}$ . We can now connect  $\gamma(t_1)$  to a point in  $B \cap \mathcal{S}$  by a s-a path inside  $\overline{B} \cap \mathcal{S}$  using (1).

- (3)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$ ,  $\mathcal{C}(W_b^{(p)}, x) \subset \overline{B}$  and  $b \in \mathcal{D}^{(p)}$ :

Since  $b \in \mathcal{D}^{(p)}$  by Property 3.2 (3) there exists  $x' \in \mathcal{C}(W_b^{(p)}, x) \cap \mathcal{M}^{(p)}$ . Thus, there exists a s-a path connecting  $x$  to  $x' \in \mathcal{M}^{(p)}$  with image contained in  $\overline{B} \cap W^{(p)} \subset \overline{B} \cap \mathcal{S}$ . We can now connect  $x'$  to a point in  $B \cap \mathcal{S}$  by a s-a path inside  $\overline{B} \cap \mathcal{S}$  using (1).

- (4)  $x \notin \mathcal{M} \cup \mathcal{M}^{(p)}$ ,  $\mathcal{C}(W_b^{(p)}, x) \subset \overline{B}$  and  $b \notin \mathcal{D}^{(p)}$ :

Since  $b \notin \mathcal{D}^{(p)}$ , for all  $a < b$  such that  $[a, b] \cap \mathcal{D}^{(p)} = \emptyset$ ,  $\mathcal{C}(W_{[a, b]}^{(p)}, x)_b = \mathcal{C}(W_b^{(p)}, x)$  and  $\mathcal{C}(W_{[a, b]}^{(p)}, x)_a \neq \emptyset$  by Property 3.2 (3). Let  $x' \in \mathcal{C}(W_{[a, b]}^{(p)}, x)_a$ . We can choose a s-a path  $\gamma : [0, 1] \rightarrow \mathcal{C}(W_{[a, b]}^{(p)}, x)$  with  $\gamma(0) = x, \gamma(1) = x'$ . Let

$$t_1 = \max\{0 \leq t < 1 \mid \gamma(t) \in W_b^{(p)}\}.$$

Then, either  $\gamma(t_1) \in \mathcal{M}$  and we can connect  $\gamma(t_1)$  to a point in  $B \cap \mathcal{S}$  by a s-a path inside  $\overline{B} \cap \mathcal{S}$  using (1). Otherwise, by Lemma 3.6 (2 b), for all small enough  $r > 0$ ,  $\mathcal{B}_k(\gamma(t_1), r) \cap C_{< b}$  is non-empty and contained in  $B$ . Then, there exists  $t_2 \in (t_1, 1]$  such that  $\gamma(t_2) \in B \cap W^{(p)} \subset B \cap \mathcal{S}$ , and the s-a path  $\gamma|_{[0, t_2]}$  gives us the required path in this case.

Take  $x$  and  $x'$  in  $\overline{B} \cap \mathcal{S}$ . They can be connected to points  $z$  and  $z'$  in  $B \cap \mathcal{S}$  by s-a paths  $\gamma$  and  $\gamma'$  inside  $\overline{B} \cap \mathcal{S}$  such that, without loss of generality,  $\pi_1(z) = \pi_1(z') = a$  with  $a < b$ , and  $b - a$  arbitrarily small. Since  $B$  is a s-a connected component of  $C_{<b}$ , it follows from Hardt's s-a triviality theorem [2, Theorem 5.45] that for all  $a < b$  with  $b - a$  sufficiently small,  $B_{\leq a}$  is non-empty and connected, and hence  $B_{\leq a}$  is a s-a connected component of  $C_{\leq a}$ . Now, using property **P**( $a$ ), we conclude that property **P**( $b$ ) holds.

**Proof of (b)** We have to prove that  $C \cap \mathcal{S}$  is non-empty and s-a connected.

Since we suppose that  $\dim(C) > 0$ ,  $C_{<b}$  is non-empty by Lemma 3.6 (2). Let  $B$  be a s-a connected component of  $C_{<b}$ . We have from (a) that  $\overline{B} \cap \mathcal{S}$  is non-empty, and since  $\overline{B} \subset C$ , it follows that  $C \cap \mathcal{S}$  is not empty.

We now prove that  $C \cap \mathcal{S}$  is s-a connected. Let  $x$  and  $x'$  be in  $C \cap \mathcal{S}$ . We prove that it is possible to connect them by a s-a path inside  $C \cap \mathcal{S}$ . Using Lemma 3.6 (2c), let  $B_i$  (resp.  $B_j$ ) be a s-a connected component of  $C_{<b}$  such that  $x \in \overline{B}_i$  (resp.  $x' \in \overline{B}_j$ ).

If  $i = j$ ,  $x$  and  $x'$  both lie in  $\overline{B}_i \cap \mathcal{S}$  which is s-a connected by (a). Hence, they can be connected by a s-a connected path in  $\overline{B}_i \cap \mathcal{S} \subset C \cap \mathcal{S}$ .

So let us suppose that  $i \neq j$ . Note that:

- by Lemma 3.6 (2a),  $\overline{B}_i \cap \mathcal{M}$  and  $\overline{B}_j \cap \mathcal{M}$  are not empty,
- by (a)  $\overline{B}_i \cap \mathcal{S}$  and  $\overline{B}_j \cap \mathcal{S}$  are s-a connected,
- by definition of  $\mathcal{S}$ ,  $\mathcal{M} \subset \mathcal{S}$ .

Then, one can connect  $x$  (resp.  $x'$ ) to a point in  $\overline{B}_i \cap \mathcal{M}$  (resp.  $\overline{B}_j \cap \mathcal{M}$ ). This shows that one can suppose without loss of generality that  $x \in \overline{B}_i \cap \mathcal{M}$  and  $x' \in \overline{B}_j \cap \mathcal{M}$ .

Let  $\gamma : [0, 1] \rightarrow C$  be a s-a path that connects  $x$  to  $x'$ , and let  $G = \gamma^{-1}(C \cap \mathcal{M})$  and  $H = [0, 1] \setminus G$ .

Since  $\mathcal{M}$  is finite, we can assume without loss of generality that  $G$  is a finite set of points, and  $H$  is a union of a finite number of open or half-open intervals.

Since  $\gamma(G) \subset \mathcal{M} \subset \mathcal{S}$ , it suffices to prove that if  $t$  and  $t'$  are the end points of an interval in  $H$ , then  $\gamma(t)$  and  $\gamma(t')$  are connected by a s-a path inside  $C \cap \mathcal{S}$ .

Notice that  $\gamma((t, t')) \cap \mathcal{M} = \emptyset$ , so that  $\gamma(t)$  and  $\gamma(t')$  belong to the same  $\overline{B}_\ell$  by Lemma 3.6 (2b). Recall now that  $\gamma(t)$  and  $\gamma(t')$  both lie in  $\overline{B}_\ell \cap \mathcal{S}$  and that  $\overline{B}_\ell \cap \mathcal{S}$  is s-a connected by (a). Consequently,  $\gamma(t)$  and  $\gamma(t')$  can be connected by a s-a path in  $\overline{B}_\ell \cap \mathcal{S} \subset C \cap \mathcal{S}$ .  $\square$

We are going to need the following corollary.

**Corollary 3.9.** *Let*

$$(V, \mathcal{M}, W^{(p)}, \mathcal{M}^{(p)}, \mathcal{D}^{(p)})$$

*satisfy Property 3.2,*

$$\mathcal{N} = \pi_{[1,p]}(\mathcal{M}), \mathcal{N}^{(p)} = \pi_{[1,p]}(\mathcal{M}^{(p)}),$$

*and  $\mathcal{N}' \subset \mathbb{R}^p$  a finite set containing  $\mathcal{N} \cup \mathcal{N}^{(p)}$ . For every s-a connected component  $C$  of  $V$ ,*

$$C \cap (W^{(p)} \cup V_{\mathcal{N}'})$$

*is s-a connected.*

*Proof.* Follows immediately from Proposition 3.3 and Property 3.2 b).  $\square$



## 4. BLOCK REPRESENTATIONS AND CURVE SEGMENTS

We denote by  $D$  an ordered domain contained in a real closed field  $R$  and by  $C$  the algebraically closed field  $R[\sqrt{-1}]$ . All the polynomials in the input and output of our algorithms have coefficients in  $D$  and the complexity of our algorithms is measured by the number of arithmetic operations (addition, multiplication, sign determination) in  $D$ .

In this section, we first define certain representations of points, as well as of s-a curves, that are going to be used in the inputs and outputs of our algorithms. Several of these representations share the common property that a certain initial number of coordinates are fixed by a triangular system of equations, along with certain Thom encodings and the remaining coordinates are defined by rational functions to be evaluated at a fixed real root of another polynomial (see Definitions 4.1 and 4.8 below). The structure of these representations reflect the recursive structure of our main algorithms described in Section 7.

After defining these representations, we recall the input, output and an upper bound on the complexity of a key algorithm, Algorithm 1 (Curve Segments), which is described in full detail in [3]. Algorithm 1 accepts as input a polynomial defining a bounded real algebraic variety (with some coordinates fixed by a triangular system as mentioned above), and outputs a s-a partition of the first (non-fixed) coordinate, as well as descriptions of s-a curve segments (as well as points) parametrized by this coordinate satisfying certain properties – which are the key to the construction of the main roadmap algorithm. Indeed, the curve segments appearing in the output of the main roadmap algorithm (Algorithm 7) are limits of the curve segments output by the various calls to Algorithm 1.

We begin with a few definitions.

**Definition 4.1.** A *Thom encoding*  $f, \sigma$  representing an element  $\alpha \in R$  consists of

- (1) a polynomial  $f \in D[T]$  such that  $\alpha$  is a root of  $f$  in  $R$ ,
- (2) a sign condition  $\sigma$  on the set  $\text{Der}(f)$  of derivatives of  $f$ , such that  $\sigma$  is the sign condition satisfied by  $\text{Der}(f)$  at  $\alpha$ .

If  $(f, \sigma)$  is a Thom encoding representing an element  $\alpha \in R$ , we will sometimes abuse notation slightly and say that  $\sigma$  is the Thom encoding of the real root  $\alpha$  of  $f$ .

Distinct roots of  $f$  in  $R$  correspond to distinct Thom encodings [2, Proposition 2.28].

A *real univariate representation*  $g, \tau, G$  representing  $x \in R^k$  consists of

- (1) a Thom encoding  $g, \tau$  representing an element  $\beta \in R$ ,
- (2)  $G = (g_0, g_1, \dots, g_k) \in D[T]^{k+1}$  where  $g$  and  $g_0$  are co-prime and such that

$$x = \left( \frac{g_1(\beta)}{g_0(\beta)}, \dots, \frac{g_k(\beta)}{g_0(\beta)} \right) \in R^k.$$

**4.1. Block representations.** In our algorithms, we make recursive calls, where we fix blocks of several coordinates. This makes necessary the following rather technical definitions.

**Definition 4.2.** A *triangular Thom encoding*  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]}), \sigma$  representing  $t = (t_1, \dots, t_m)$  in  $R^m$  consists of

- (1) a triangular system  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$ , i.e.  $f_{[i]} \in D[T_1, \dots, T_i]$  for  $i = 1, \dots, m$ , such that the zero set of  $\mathcal{F}$  in  $C^m$  is finite;



- (2) a list,  $\sigma = (\sigma_1, \dots, \sigma_m)$ , where for  $i = 1, \dots, m$ ,  $\sigma_i$  is the Thom encoding of the root  $t_i$  of  $f_{[i]}(t_1, \dots, t_{i-1}, T_i)$ .

A triangular system  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$  is *quasi-monic* if the leading coefficient of  $f_{[i]} \in D[T_1, \dots, T_i]$  with respect to  $T_i$  is a strictly positive element in  $D$  and  $\deg_{T_i}(f_{[j]}) < \deg_{T_i}(f_{[i]})$ ,  $j > i$ . A triangular Thom encoding  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$ ,  $\sigma$  is *quasi-monic* if  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$  is quasi-monic.

Let  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$  be a quasi-monic triangular system. Let  $c \in D$ ,  $c$  strictly positive and  $g \in D[T_1, \dots, T_m]$ , we say that  $cg$  has a *reduction in  $D$  modulo  $\mathcal{F}$*  if there exists a polynomial  $\bar{g} \in D[T_1, \dots, T_m]$  such that  $\deg_{T_i}(\bar{g}) < \deg_{T_i}(f_{[i]})$  for  $i = 1, \dots, m$  and

$$cg = \bar{g} \pmod{I(\mathcal{F})},$$

where  $I(\mathcal{F})$  is the ideal of  $D[T_1, \dots, T_m]$  generated by  $f_{[1]}, \dots, f_{[m]}$ . The polynomials  $\bar{g}$  is unique with these properties since a quasi-monic triangular system is a Groebner basis with respect to the lexicographical ordering. We say that the couple  $(c, \bar{g})$  is a *pseudo-reduction of  $g$* .

Note that at the zeros of  $\mathcal{F}$  the signs of  $g$  and  $\bar{g}$  coincide.

**Remark 4.3.** If  $g \in D[T_1, \dots, T_m]$  is a polynomial of degree  $D$ , and  $d$  is a bound on the degree of the  $f_i$  with respect to the  $T_i$ , the complexity of computing a pseudo-reduction  $(c, \bar{g})$  of  $g \in D[T_1, \dots, T_m]$  modulo  $\mathcal{F}$  is  $(Dd)^{O(m)}$  (see Section 8 Proposition 8.4 a)).

**Definition 4.4.** A *real block representation  $\mathcal{F}, \sigma, L, F$  representing  $y \in \mathbb{R}^\ell$*  consists of

- (1) a triangular Thom encoding  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]})$ ,  $\sigma$  representing a root  $t = (t_1, \dots, t_m)$  of  $\mathcal{F}$  in  $\mathbb{R}^m$ ;
- (2) a list of natural numbers  $L = (\ell_1, \dots, \ell_m)$  such that

$$\ell = \ell_1 + \dots + \ell_m;$$

- (3) a list of polynomials  $F = (F_{[1]}, \dots, F_{[m]})$ , where

$$F_{[i]} = (f_{[i]0}, \dots, f_{[i]\ell_i}), f_{[i]j} \in D[T_1, \dots, T_i], 0 \leq j \leq \ell_i,$$

with  $f_{[i]}(t_1, \dots, t_{i-1}, T_i), f_{[i]0}(t_1, \dots, t_{i-1}, T_i)$  coprime (as polynomials in  $T_i$ ), such that

$$y = (y_{[1]}, \dots, y_{[m]}) \in \mathbb{R}^\ell,$$

with

$$y_{[i]} = \left( \frac{f_{[i]1}(t_1, \dots, t_i)}{f_{[i]0}(t_1, \dots, t_i)}, \dots, \frac{f_{[i]\ell_i}(t_1, \dots, t_i)}{f_{[i]0}(t_1, \dots, t_i)} \right), 1 \leq i \leq m.$$

In the case  $\ell_1 = \dots = \ell_m = p$  we will write

$$L = [p^m]. \tag{4.1}$$

**Notation 4.5** (Substituting a real block representation in a polynomial). Let  $\mathcal{F}, \sigma, L, F$  be a real block representation representing  $y \in \mathbb{R}^\ell$ , and let  $t \in \mathbb{R}^m$  be represented by  $\mathcal{F}, \sigma$ .

Let

$$\bar{f}_{[i]}(T_1, \dots, T_i) = \left( \frac{f_{[i]1}(T_1, \dots, T_i)}{f_{[i]0}(T_1, \dots, T_i)}, \dots, \frac{f_{[i]\ell_i}(T_1, \dots, T_i)}{f_{[i]0}(T_1, \dots, T_i)} \right).$$

Given  $Q \in D[X_1, \dots, X_k]$  with  $\ell \leq k$ , we set  $T = (T_1, \dots, T_m)$ , and define  $Q_F \in D[T, X_{\ell+1}, \dots, X_k]$  by

$$Q_F := \bar{f}_0(T)Q(\bar{f}_{[1]}(T_1), \dots, \bar{f}_{[m]}(T_1, \dots, T_m), X_{\ell+1}, \dots, X_k), \quad (4.2)$$

where

$$\bar{f}_0(T) = \prod_{i=1}^m f_{[i]0}(T_1, \dots, T_i)^{e_i},$$

and  $e_i$  is the smallest even number  $\geq \deg_{X_{[i]}}(Q)$ , where  $X_{[i]}$  is the block of variables  $X_{\ell_1+\dots+\ell_{i-1}+1}, \dots, X_{\ell_1+\dots+\ell_i}$ .

Note that

$$Q_F(t, X_{\ell+1}, \dots, X_k) = \bar{f}_0(t)Q(y, X_{\ell+1}, \dots, X_k),$$

with  $\bar{f}_0(t) > 0$ . More generally, for any family of polynomials  $\mathcal{Q} \subset D[X_1, \dots, X_k]$  with  $\ell \leq k$ , we will denote  $\mathcal{Q}_F = \{Q_F \mid Q \in \mathcal{Q}\}$ .

**Notation 4.6** (Substituting a real block representation in a parametrized univariate representation). Let  $\mathcal{F}, \sigma, L, F$  be as above and let  $g, G$  with  $G = (g_0, g_{\ell+1}, \dots, g_k)$ , be a parametrized univariate representation, i.e.  $g, g_0, g_{\ell+1}, \dots, g_k \in D[X_1, \dots, X_\ell, U]$ , where  $X_1, \dots, X_\ell$  are the parameters, and  $U$  a single variable.

We denote by  $G_F$  the tuple  $(g_{0,F}, \dots, g_{k,F})$ , where each  $g_{i,F} \in D[T, U]$  and is defined by

$$g_{i,F} := \bar{f}_0(T)g_i(\bar{f}_{[1]}(T_1), \dots, \bar{f}_{[m]}(T_1, \dots, T_m), X_{\ell+1}, \dots, X_k), \quad (4.3)$$

where

$$\bar{f}_0(T) = \prod_{i=1}^m f_{[i]0}(T_1, \dots, T_i)^{e_i},$$

and  $e_i$  is the smallest even number  $\geq \max_j \deg_{X_{[i]}}(g_j)$ .

**Definition 4.7.** Let  $t \in \mathbb{R}^m$  be represented by a triangular Thom encoding  $\mathcal{F}, \sigma$ .

A *Thom encoding*  $g, \tau$  representing  $\beta$  over  $t$  consists of (using the same notation as above)

- (1) a polynomial  $g \in D[T_1, \dots, T_m, T]$  such that  $g(t, \beta) = 0$ ,
- (2) a sign condition  $\tau$  on  $\text{Der}_T(g)$  such that  $\tau$  is the sign condition satisfied by the set  $\text{Der}_T(g(t, T))$  at  $\beta$ .

A *real univariate representation* representing  $x \in \mathbb{R}^k$  over  $t$  consists of

- (1) a Thom encoding  $g, \tau$  representing  $\beta$  over  $t$ ,
- (2)  $G = (g_0, g_1, \dots, g_k) \in D[T_1, \dots, T_m, U]^{k+1}$  such that  $g(t, U), g_0(t, U)$  are coprime, and such that

$$x = \left( \frac{g_1(t, \beta)}{g_0(t, \beta)}, \dots, \frac{g_k(t, \beta)}{g_0(t, \beta)} \right) \in \mathbb{R}^k.$$

A real univariate representation over  $t$  is *quasi-monic* if the leading monomial of  $g$  with respect to  $U$  is in  $D$ .

A *triangular Thom encoding* representing  $z = (z_1, \dots, z_r)$  over  $t$  with variables  $Z_1, \dots, Z_r$  consists of

- (1) a triangular system  $\mathcal{H} = (h_1, \dots, h_r)$ , with

$$h_i \in D[T_1, \dots, T_m, Z_1, \dots, Z_i]$$

for  $i = 1, \dots, r$ , such that the zero set of  $\mathcal{H}(t, Z_1, \dots, Z_r)$  in  $\mathbb{C}^r$  is finite;

- (2) a list,  $\rho = (\rho_1, \dots, \rho_r)$ , where for  $i = 1, \dots, r$ ,  $\rho_i$  is the Thom encoding of the root  $z_i$  of  $h_i(t, z_1, \dots, z_{i-1}, Z_i)$ .

#### 4.2. Curve segments.

**Definition 4.8.** Let  $t \in \mathbb{R}^m$  be represented by a triangular Thom encoding  $\mathcal{F}, \sigma$ . A curve segment with parameter  $X_j$  over  $t$  on  $(\alpha_1, \alpha_2)$  in  $\mathbb{R}^k$ ,

$$f_1, \sigma_1, f_2, \sigma_2, g, \tau, G$$

is given by

- (1)  $\alpha_1, \alpha_2 \in \mathbb{R}$  represented by Thom encodings  $f_1, \sigma_1$  and  $f_2, \sigma_2$  over  $t$ ;
- (2) a parametrized univariate representation with parameter  $X_j$ , i.e.

$$g, G = (g_0, g_1, \dots, g_k),$$

with  $g_j = X_j g_0$  and  $g, g_0, \dots, g_k$  in  $D[T_1, \dots, T_m, X_j, U]$ ;

- (3) a sign condition  $\tau$  on  $\text{Der}_U(g)$  such that for every  $x_j \in (\alpha_1, \alpha_2)$  there exists a real root  $u(x_j)$  of  $g(t, x_j, U)$  with Thom encoding  $\tau$ , and  $g_0(t, x_j, u(x_j)) \neq 0$ .

The curve represented by  $f_1, \sigma_1, f_2, \sigma_2, g, \tau, G$  is the image of the smooth injective s-a function  $\gamma$  which maps a point  $x_j$  of  $(\alpha_1, \alpha_2)$  to the point of  $\mathbb{R}^k$  defined by

$$\gamma(x_j) = \left( \frac{g_1(t, x_j, u(x_j))}{g_0(t, x_j, u(x_j))}, \dots, \frac{g_k(t, x_j, u(x_j))}{g_0(t, x_j, u(x_j))} \right).$$

Let  $Q \in R[X_1, \dots, X_k]$ . For  $0 \leq \ell < k$  and  $y \in \mathbb{R}^\ell$ , we write

$$Q(y, -) \stackrel{\text{def}}{=} Q(y_1, \dots, y_\ell, X_{\ell+1}, \dots, X_k). \quad (4.4)$$

*Remark 4.9.* Abusing notation slightly, we will occasionally identify

$$\text{Zer}(Q(y, -), \mathbb{R}^{k-\ell}) \subset \mathbb{R}^{k-\ell}$$

with

$$\{y\} \times \text{Zer}(Q(y, -), \mathbb{R}^{k-\ell}) = \text{Zer}(Q, \mathbb{R}^k)_y \subset \mathbb{R}^k.$$

More generally, for a s-a set  $A \subset \mathbb{R}^k$ , we will occasionally identify  $\{x \in \mathbb{R}^{k-\ell} \mid (y, x) \in A_y\}$  with  $A_y \subset \mathbb{R}^k$ .

We now recall the input, output and complexity of [3, Algorithm 15.2 (Curve segments)].

#### ALGORITHM 1. [Curve Segments]

- INPUT. (1) a point  $t \in \mathbb{R}^m$  represented by a triangular Thom encoding  $\mathcal{F}, \sigma$ ;  
 (2) a polynomial  $P \in D[T_1, \dots, T_m, X_1, \dots, X_k]$  for which  $\text{Zer}(P(t, -), \mathbb{R}^k)$  is bounded;  
 (3) a finite set of points contained in  $\text{Zer}(P(t, -), \mathbb{R}^k)$  represented by real univariate representations  $\mathcal{U}$  over  $t$ .

Moreover, all the polynomials describing the input are with coefficients in  $D$ .

- OUTPUT. (1) An ordered list of points  $c_1 < \dots < c_N$  of  $\mathbb{R}$  with each  $c_i$   $i = 1, \dots, N$  represented by a Thom encoding  $g_i, \tau_i$  over  $t$ . The  $c_i$ 's are called *distinguished values*.  
 (2) For every  $i = 1, \dots, N$ , a finite set of real univariate representations  $\mathcal{D}_i$  over  $t$  representing a finite number of points in  $\mathbb{R}^k$ , called *distinguished points*.

- (3) For every  $i = 1, \dots, N-1$  a finite set of curve segments  $\mathcal{C}_i$  defined on  $(c_i, c_{i+1})$  with parameter  $X_1$ , over  $t$ . The represented curves are called *distinguished curves*.
- (4) For every  $i = 1, \dots, N-1$  a list of pairs of elements of  $\mathcal{C}_i$  and  $\mathcal{D}_i$  (resp.  $\mathcal{D}_{i+1}$ ) describing the adjacency relations between distinguished curves and distinguished points.

The distinguished curves and points are contained in  $\text{Zer}(P(t, -), \mathbb{R}^k)$ . The sets of distinguished values, distinguished curves, and distinguished points satisfy the following properties.

CS<sub>1</sub>. If  $c \in \mathbb{R}$  is a distinguished value, the set of distinguished points in the output intersect every s-a connected component of

$$\text{Zer}(P(t, c, -), \mathbb{R}^{k-1}).$$

If  $c \in \mathbb{R}$  is not distinguished, the distinguished curves in the output intersect every s-a connected component of

$$\text{Zer}(P(t, c, -), \mathbb{R}^{k-1}).$$

CS<sub>2</sub>. For each distinguished curve in the output over an interval with endpoint a given distinguished value, there exists a distinguished point over this distinguished value which belongs to the closure of the curve.

COMPLEXITY. If  $d = \deg_X(P) \geq 2$ ,  $\deg_T(P) = D$ , and the degree of the polynomials in  $\mathcal{F}$  and the number of elements of  $\mathcal{U}$  are bounded by  $D$ , the number of arithmetic operations in  $\mathbb{D}$  is bounded by  $D^{O(m)}d^{O(mk)}$ . Moreover, the degree in  $T_i$  of the polynomials appearing in the output is bounded by  $Dd^{O(k)}$ .

## 5. LOW DIMENSIONAL ROADMAP IN A SPECIAL CASE

In this section we describe an algorithm for computing the roadmap of a variety described by equations having a special structure. Although, this algorithm is very similar to [2, Algorithm 15.3 (Bounded Algebraic Roadmap)], the complexity analysis differs because of the special structure assumed for the input.

Let  $Q \in \mathbb{R}[X_1, \dots, X_k]$  and suppose that  $V = \text{Zer}(Q, \mathbb{R}^k)$  is bounded.

For  $0 \leq \ell < k$ ,  $0 \leq p \leq k - \ell$ , and  $y \in \mathbb{R}^\ell$ , we write

$$\text{Cr}_{\ell+p}(Q)(y, -) \stackrel{\text{def}}{=} \left( Q(y, -), \frac{\partial Q}{\partial X_{\ell+p+2}}(y, -), \dots, \frac{\partial Q}{\partial X_k}(y, -) \right). \quad (5.1)$$

We assume that  $Q$  satisfies the following property.

**Property 5.1.** For every  $\ell$ ,  $0 \leq \ell < k$ ,  $0 \leq p < k - \ell$ , and  $y \in \mathbb{R}^\ell$ , the algebraic set

$$W_y^{(p)} = \text{Zer}(\text{Cr}_{\ell+p}(Q)(y, -), \mathbb{R}^{k-\ell})$$

is of dimension  $p$  or empty.

*Remark 5.2.* Note that for every  $y \in \mathbb{R}^\ell$ ,  $z \in \mathbb{R}^r$ ,  $(W_y^{(r)})_z = W_{(y,z)}^{(0)}$  has a finite number of points and, since  $V$  is bounded, intersects every s-a connected component of  $V_{(y,z)}$  by [3, Proposition 7.4].

**Proposition 5.3.** Suppose that  $V$  is bounded and  $Q$  satisfies Property 5.1. Let

- (1)  $\mathcal{M} = W_y^{(0)} \subset V_y$ ;

- (2)  $\mathcal{D}^{(p)} \subset \mathbb{R}$  the set of pseudo-critical values (see [2, Definition 12.41]) of  $\pi_{\ell+1}$  on  $W_y^{(p)}$ , and  $\mathcal{M}^{(p)}$  a set of points such that for every  $c \in \mathcal{D}^{(p)}$ ,  $\mathcal{M}^{(p)}$  intersects every  $s$ -a connected component  $D$  of  $(W_y^{(p)})_c$ .

Then,

$$\left( V_y, \mathcal{M}, W_y^{(p)}, \mathcal{M}^{(p)}, \mathcal{D}^{(p)} \right)$$

satisfies Property 3.2.

*Proof.* Note that by Property 5.1,  $W_y^{(p)}$  is of dimension  $p$  or empty. In particular,  $W_y^{(0)}$  is finite, i.e. zero-dimensional or empty, and satisfies Property 3.2 2): for each  $z \in \mathbb{R}^p$ ,  $(W_y^{(p)})_z = W_{(y,z)}^{(0)}$  is a finite set of points having non-empty intersection with every  $s$ -a connected component of  $V_{(y,z)}$  by Remark 5.2. Moreover,  $\text{Zer}(Q(y, -), \mathbb{R}^{k-\ell})$  is clearly bounded (since  $\text{Zer}(Q, \mathbb{R}^k)$  is bounded), and the finite set  $\mathcal{M} = W_y^{(0)}$  is the union of the  $Q(y, -)$ -singular points of  $\text{Zer}(Q(y, -), \mathbb{R}^{k-\ell})$  and the  $Q(y, -)$ -critical points of the map  $\pi_{\ell+1}$  on  $V_y = \text{Zer}(Q(y, -), \mathbb{R}^{k-\ell})$ . Thus,  $\mathcal{M}$  satisfies Property 3.2 1).

Note also that  $\mathcal{M}^{(p)}$  satisfies Property 3.2 3). Indeed, the intersection of  $\mathcal{M}^{(p)}$  with every  $s$ -a connected component of  $(W_y^{(p)})_c$  is non-empty, by [2, Proposition 12.42]. Moreover for every interval  $[a, b]$  and  $c \in [a, b]$  such that  $[a, b]$  contains no point of  $\mathcal{D}^{(p)}$ , except maybe  $c$ , and for every  $s$ -a connected component  $C$  of  $(W_y^{(p)})_{[a,b]}$ ,  $C_{(y,c)}$  is a  $s$ -a connected component of  $(W_y^{(p)})_c$ , by [2, Proposition 15.4].  $\square$

We are going to describe below, in the special case where  $Q$  defines a bounded real algebraic set and satisfies Property 5.1, an algorithm directly adapted from [2, Algorithm 15.3] for computing a roadmap of certain subvarieties of  $\text{Zer}(Q, \mathbb{R}^k)$  of dimension at most  $p$ : this is Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets).

*Remark 5.4.* In all our algorithms, the roadmaps output are represented by a finite number of real univariate representations and curve segments over a point defined by a triangular Thom encoding (see Definitions 4.4, 4.7, and 4.8 above).

**ALGORITHM 2. [Roadmap for Lower Dimensional Special Algebraic Sets]**

- INPUT. (1) a polynomial  $Q \in \mathbb{D}[X_1, \dots, X_k]$  satisfying Property 5.1, and for which  $V = \text{Zer}(Q, \mathbb{R}^k) \subset \mathcal{B}_k(0, 1/c)$  (where  $c \in \mathbb{R}$ );  
 (2) natural numbers  $p, m, r \geq 0$  satisfying  $0 \leq k - mp \leq p, 0 \leq r < p$ ;  
 (3)  $y \in \mathbb{R}^{mp}$  represented by a real block representation  $\mathcal{F}, \sigma, [p^m], F$  (see (4.1)) with  $t \in \mathbb{R}^m$  represented by a quasi-monic triangular system  $\mathcal{F}, \sigma$ ;  
 (4)  $z \in \mathbb{R}^r$  represented by a triangular Thom encoding  $\mathcal{H}, \rho$  over  $t$ , with variables  $X_{mp+1}, \dots, X_{mp+r}$ ;  
 (5) a finite set of points  $\mathcal{M}_0$  contained in

$$W_{(y,z)}^{(p-r)} = \text{Zer}(\text{Cr}_{(m+1)p}(Q)(y, z, -), \mathbb{R}^{k-(mp+r)})$$

represented by real univariate representations  $\mathcal{U}_0$ , over  $(t, z)$  (using the notation of Property 5.1).

OUTPUT. a roadmap  $\text{RM}(W_{(y,z)}^{(p-r)}, \mathcal{M}_0)$  for  $(W_{(y,z)}^{(p-r)}, \mathcal{M}_0)$  represented as a union of curve segment representations and real univariate representations over points defined by triangular Thom encodings. The adjacencies between the images of the associated curves and points are also part of the output.

COMPLEXITY.  $D^{O(m+p)}d^{O((m+p)k)}$  where  $d = \deg(Q) \geq 2$ , and  $D$  is a bound on the degree of  $\mathcal{H}, \mathcal{F}, F$  and the number and degrees of the elements in  $\mathcal{U}_0$ .

PROCEDURE.

Step 0. If  $mp + r \geq k$  then exit. Else do the following.

Step 1. Denote

$$P := \sum_{A \in \text{Cr}_{(m+1)p}(Q)_F} A^2 \in \text{D}[T_1, \dots, T_m, X_{mp+1}, \dots, X_k]$$

using Notation 4.5 and (5.1). Call Algorithm 1 (Curve Segments) with input

$$(\mathcal{F}, \mathcal{H}), (\sigma, \rho), P, \mathcal{U}_0.$$

Compute a pseudo-reduction of the output of the call to Algorithm 1 (Curve Segments) in the previous step modulo  $\mathcal{F}$  (using Proposition 8.4), and place the result in the description of  $\text{RM}(W_{(y,z)}^{(p-r)}, \mathcal{M}_0)$ .

Step 2. Using the notation in the output of Algorithm 1, for every  $j = 1, \dots, N$ , define

$$\begin{aligned} z &:= (z, c_j), \\ \mathcal{H} &:= (\mathcal{H}, g_j(T_1, \dots, T_m, X_1, \dots, X_{r+i})), \\ \rho &:= (\rho, \tau_j), \\ \mathcal{U}_0 &:= \mathcal{D}_j, \end{aligned}$$

and call Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets) recursively, with input

$$(Q, (p, m, r+1), (\mathcal{F}, \sigma, [p^m], F), (\mathcal{H}, \rho), \mathcal{U}_0).$$

Include in the description of  $\text{RM}(W_{(y,z)}^{(p-r)}, \mathcal{M}_0)$ , the output of the call.

PROOF OF CORRECTNESS. Notice that

$$W_{(y,z)}^{(p-r)} = \text{Zer}(P(t, z, -), \mathbb{R}^{k-(mp+r)}).$$

The correctness of the algorithm then follows from the correctness of Algorithm 1 (Curve Segments) and Proposition 2.2. The only additional fact that needs to be checked is that when the recursion ends with  $r = k - mp \leq p$ , the algebraic variety  $\text{Zer}(P((t, z, z'), -), \mathbb{R}^{k-p(m+1)})$  is finite, where  $z' = (c_{j_1}, \dots, c_{j_{p-r}}) \in \mathbb{R}^{p-r}$  and the various  $c_{j_i} \in \mathbb{R}$  are associated to the Thom encodings computed in Step 1 of the algorithm. This is the case because  $\text{Zer}(P((t, z, z'), -), \mathbb{R}^{k-p(m+1)}) = W_{(y,z,z')}^{(0)}$ , and  $W_{(y,z,z')}^{(0)}$  is finite by Property 5.1.  $\square$

COMPLEXITY ANALYSIS. The depth  $i$  of the recursion is bounded by  $p - r$ , and the total number of recursive calls at depth  $i$  is bounded by  $d^{O(ik)}$ . Thus, there are at most  $d^{O((p-r)k)}$  calls to Algorithm 1 (Curve Segments).

In each of the calls to Algorithm 1 (Curve Segments), the number of arithmetic operations in  $\text{D}$  is bounded by  $D^{O(m+p)}d^{O((m+p)k)}$  using the complexity analysis

of Algorithm 1 (Curve Segments). Moreover the number of arithmetic operations needed for each pseudo-reduction is  $(Dd^k)^{O(m)}$  since the degree in  $T_i$  of the output of Algorithm 1 (Curve Segments) is  $Dd^{O(k)}$  using Remark 4.3.

Thus, the total number of arithmetic operations in  $\mathbb{D}$  for Algorithm 2 is bounded by  $D^{O(m+p)}d^{O((m+p)k)}$ .  $\square$

## 6. LOW DIMENSIONAL ROADMAP IN GENERAL

In this section, we first explain how to perform an infinitesimal deformation of any given polynomial  $Q \in \mathbb{R}[X_1, \dots, X_k]$  such that the deformed polynomial satisfies Property 5.1.

We then sketch how to compute the limit of a curve. We also describe how to compute the limits of roadmaps of certain algebraic sets which are the critical locus of dimension  $p$  of certain projection maps restricted to the algebraic hypersurfaces obtained after performing an infinitesimal deformation.

**6.1. Deformation.** We consider a bounded algebraic set defined by a non-negative polynomial  $Q$ . Our aim is to define an infinitesimal deformation of  $Q$  such that the deformed polynomial satisfies Property 5.1. Suppose that the polynomial  $Q \in \mathbb{R}[X_1, \dots, X_k]$  and the tuple  $(d_1, \dots, d_k)$  satisfy the following additional conditions:

- (1)  $d_1 \geq d_2 \geq \dots \geq d_k$ ,
- (2)  $\deg(Q) \leq d_1$ ,  $\text{tDeg}_{X_i}(Q) \leq d_i$ , for  $i = 2, \dots, k$ , where  $\text{tDeg}_{X_i}(Q)$  is the maximum degree amongst all monomials in  $Q$  containing  $X_i$ .

Let  $\bar{d}_i$  be an even number  $> d_i$ ,  $i = 1, \dots, k$ , and  $\bar{d} = (\bar{d}_1, \dots, \bar{d}_k)$ . Let

$$G_k(\bar{d}) = X_1^{\bar{d}_1} + \dots + X_k^{\bar{d}_k} + X_2^2 + \dots + X_k^2 + X_{k+1}^2 + 2k,$$

and note that for all  $x \in \mathbb{R}^{k+1}$   $G_k(\bar{d})(x) > 0$ .

We denote for ever  $\ell$ ,  $0 \leq \ell \leq k$  and every  $y \in \mathbb{R}^\ell$ :

**Notation 6.1.**

$$\begin{aligned} \text{Def}(Q, \varepsilon) &= -\varepsilon G_k(\bar{d}) + Q, \\ V(\varepsilon)_y &= \text{Zer}(\text{Def}(Q, \varepsilon)(y, -), \mathbb{R}\langle \varepsilon \rangle^{k+1-\ell}), \\ \text{Cr}_{\ell+p}(Q, \varepsilon)(y, \cdot) &= \left( \text{Def}(Q, \varepsilon)(y, \cdot), \frac{\partial \text{Def}(Q, \varepsilon)}{\partial X_{p+\ell+1}}(y, \cdot), \dots, \frac{\partial \text{Def}(Q, \varepsilon)}{\partial X_{k+1}}(y, \cdot) \right), \\ W(\varepsilon)_y^{(p)} &= \text{Zer}(\text{Cr}_{\ell+p}(Q, \varepsilon)(y, -), \mathbb{R}\langle \varepsilon \rangle^{k+1-\ell}). \end{aligned}$$

**Proposition 6.2.** *For every  $\ell$ ,  $0 \leq \ell \leq k$  and every  $y \in \mathbb{R}^\ell$ :*

- a)  $\text{Def}(Q, \varepsilon)$  satisfies Property 5.1;
- b)  $\lim_{\varepsilon}$  induces a 1-1 correspondence between the bounded  $s$ -a connected components of

$$V(\varepsilon)_y = \text{Zer}(\text{Def}(Q, \varepsilon)(y, -), \mathbb{R}\langle \varepsilon \rangle^{k+1-\ell})$$

and the  $s$ -a connected components of

$$V_y = \text{Zer}(Q(y, -), \mathbb{R}^{k-\ell}).$$

*Proof.* a) follows from [2, Proposition 12.44] and b) from [2, Lemma 15.6].  $\square$

We are going to describe in Section 6.3 an algorithm for computing the limit of a roadmap of the critical locus of dimension  $p$ ,  $W(\varepsilon)_y^{(p)}$ , of  $V(\varepsilon)_y$ . In order to achieve this, we first need to compute limits of curves, which is the purpose of Section 6.2.

**6.2. Limits of points and curve segments.** The general problem of computing the image of a s-a set  $S \subset \mathbb{R}\langle\varepsilon\rangle^k$  which is bounded over  $\mathbb{R}$  under the  $\lim_\varepsilon$  map reduces to the problem of computing the closure of a one-parameter family of s-a sets, which can be done using quantifier elimination algorithms (see, for example, [2, p. 556]). However, the complexity of this general algorithm,  $d^{k^{O(1)}}$ , is not good enough for our purposes in this paper. Fortunately, we need efficient algorithms for computing limits only in two very special situations, where we can do better than in the general case.

These two special cases are the following:

- (1) when the set consists of a point represented by a real univariate representation,
- (2) when the set consists of a curve represented by curve segments.

We now describe the input, output and give an upper bound on the complexity of Algorithm 3 (Limit of a Bounded Point) and Algorithm 4 (Limit of a Curve). A full description of these algorithms, their correctness and complexity analysis appear in Section 8.

**ALGORITHM 3. [Limit of a Bounded Point]**

- INPUT. (1) a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$ , with coefficients in  $\mathbb{D}$ , representing a point  $t \in \mathbb{R}^m$ ;
- (2) a real univariate representation  $g(\varepsilon), \tau(\varepsilon), G(\varepsilon)$  over  $t$  with coefficients in  $\mathbb{D}[\varepsilon]$ , representing a point  $z(\varepsilon) \in \mathbb{R}\langle\varepsilon\rangle^p$  bounded over  $\mathbb{R}$ .
- OUTPUT. (1) a quasi-monic triangular Thom encoding  $\mathcal{F}', \sigma'$ , representing the point  $t \in \mathbb{R}^m$ ;
- (2) a quasi-monic real univariate representation  $(h, \tau, H)$  representing

$$z = \lim_\varepsilon z(\varepsilon) \in \mathbb{R}^p.$$

COMPLEXITY. If  $D_1$  (resp.  $D_2$ ) is a bound on the degrees of the polynomials in  $\mathcal{F}, g(\varepsilon)$  and  $G(\varepsilon)$  with respect to  $T_1, \dots, T_m$  (resp.  $\varepsilon, U$ ), then  $D_1$  (resp.  $D_2$ ) is a bound on the degrees of the polynomials appearing in the output, and the number of arithmetic operations in  $\mathbb{D}$  is bounded by  $D_1^{O(m)} D_2^{O(1)}$ .

*Remark 6.3.* Note that there is a possibly new representation of the point  $t \in \mathbb{R}^m$  specified in the input, in the output of Algorithm 3 (Limit of a Bounded Point). The reason for this peculiarity is explained in Section 8 (cf. Proposition 8.4 b)).

**ALGORITHM 4. [Limit of a Curve]**

- INPUT. (1) a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$  with coefficients in  $\mathbb{D}$  representing  $t \in \mathbb{R}^m$ ;
- (2) a triangular Thom encoding  $\mathcal{H}(\varepsilon), \rho(\varepsilon)$  over  $t$  with coefficients in  $\mathbb{D}[\varepsilon]$  representing  $z(\varepsilon) \in \mathbb{R}\langle\varepsilon\rangle^r$  over  $t$ ;
- (3) a curve segment with parameter  $X_{r+1}$  and coefficients in  $\mathbb{D}[\varepsilon]$  over  $(t, z(\varepsilon))$ , representing a curve  $S(\varepsilon)$  in  $\mathbb{R}\langle\varepsilon\rangle^k$  bounded over  $\mathbb{R}$ .
- OUTPUT. (1) a real univariate representation  $p_z, \rho_z, P_z$  of  $z = \lim_\varepsilon(z(\varepsilon))$ , with  $u$  the root of  $p_z$  with Thom encoding  $\rho_z$ ;
- (2) a finite set  $\mathcal{D} = \{d_1, \dots, d_{N-1}\}$  where each  $d_i$  is a real univariate representation over  $(t, u, c_i)$ , and  $c_i$  is given by a Thom encoding over  $t$  fixing  $X_{m(i)}$ ;



- (3) a finite set  $\mathcal{W} = \{w_1, \dots, w_N\}$  of curve segments over  $(t, u)$  with  $w_i$  parametrized by  $X_{\ell(i)}$ .

Moreover, the union of the curves represented by  $\mathcal{W}$ , together with the points represented by  $\mathcal{D}$  define a partition of  $S = \lim_{\varepsilon}(S(\varepsilon))$ . All the coefficients of the polynomials in the output belong to  $\mathbb{D}$ .

**COMPLEXITY** If the polynomials occurring in the input have degrees bounded by  $D$ , then the complexity of the algorithm is bounded by  $k^{O(1)}D^{O(m+r)}$ .

**6.3. Low dimensional roadmap algorithm.** We are going to describe an algorithm computing the limit of a roadmap of the critical locus of dimension  $p$ ,  $W(\varepsilon)_y^{(p)}$ , of the deformation  $V(\varepsilon)_y = \text{Zer}(\text{Def}(Q, \varepsilon)(y, -), R\langle \varepsilon \rangle^{k+1-\ell})$  of  $V_y = \text{Zer}(Q(y, -), R^{k-\ell})$ . The algorithm proceeds by first calling Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets) in order to compute a roadmap for  $W(\varepsilon)_y^{(p)}$ , and then computes the image of the resulting roadmap under the  $\lim_{\varepsilon}$  map. Note that this limit is not necessarily a roadmap of  $V_y$ , since a s-a connected component of  $V_y$  might contain the limit of more than one s-a connected component of  $W(\varepsilon)_y^{(p)}$ .

**ALGORITHM 5. [Limit of Roadmaps of Special Low Dimensional Varieties]**

- INPUT.** (1) natural numbers  $p \leq k$ ;  
 (2) a polynomial  $Q \in \mathbb{D}[X_1, \dots, X_k]$  for which  $Z = \text{Zer}(Q, R^k) \subset \mathcal{B}_k(0, 1/c)$  (with  $c \in \mathbb{R}$ );  
 (3)  $y \in \mathbb{R}^{mp}$  represented by the real block representation

$$\mathcal{F}, \sigma, [p^m], F,$$

(see (4.1)) with coefficients in  $\mathbb{D}$ , such that  $t \in \mathbb{R}^m$  is represented by a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$ ;

- (4) a finite set of points  $\mathcal{N}(\varepsilon) \in \{y\} \times \mathbb{R}\langle \varepsilon \rangle^p$  represented by quasi-monic real univariate representations  $\mathcal{V}(\varepsilon)$ , over  $t$ .

**OUTPUT.** Real univariate representations and curve segments representing the set of points

$$\mathcal{R} = (\pi_{[1,k]} \circ \lim_{\varepsilon})(\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon)))$$

where  $W(\varepsilon)_y^{(p)}$  is the zero set of  $\text{Cr}_{\ell+p}(Q, \varepsilon)(y, -)$ ,

$$\mathcal{A}(\varepsilon) = \bigcup_{z(\varepsilon) \in \mathcal{N}(\varepsilon)} W(\varepsilon)_{y, z(\varepsilon)}^{(0)}, \quad (6.1)$$

and  $\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$  is a roadmap for  $(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$ .

**COMPLEXITY.**  $D^{O(m+p)}d^{O((m+p)k)}$  where  $d = \deg(Q) \geq 2$ , and  $D$  is a bound on the degrees of  $\mathcal{F}, F$  and the number and degrees (including that in  $\varepsilon$ ) of the elements in  $\mathcal{N}(\varepsilon)$ .

**PROCEDURE.**

Step 1. Let  $T = (T_1, \dots, T_m)$ , and using Notation 4.5 and Notation 6.1,

$$P = \sum_{A \in \text{Cr}_{(m+1)p}(Q, \varepsilon)_F} A^2 \in \mathbb{D}[\varepsilon, T, X_{mp+1}, \dots, X_k].$$

Call [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] with input  $P$  and parameters  $\varepsilon, T, X_{mp+1}, \dots, X_{(m+1)p}$  and output a set of parametrized univariate representations with variable  $U$ .

Compute a pseudo-reduction of the output modulo  $\mathcal{F}$  (using Proposition 8.4) and place the result in  $\mathcal{U}(\varepsilon)$ .

For every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{U}(\varepsilon)$ , and every  $z(\varepsilon) \in \mathcal{N}(\varepsilon)$  represented by a real univariate representation  $(g(\varepsilon), \tau, G(\varepsilon)) \in \mathcal{V}(\varepsilon)$ , use [2, Algorithm 12.20 (Triangular Thom Encoding)] with input the triangular system  $(\mathcal{F}, g(\varepsilon), h(\varepsilon))$  to compute the Thom encodings of the real roots of  $h(\varepsilon)(y, z(\varepsilon), U)$ . Let  $\mathcal{U}'(\varepsilon)_{z(\varepsilon)}$  be the set of real univariate representations over  $y, z(\varepsilon)$  so obtained. Define

$$\mathcal{U}'(\varepsilon) = \bigcup_{z(\varepsilon) \in \mathcal{N}(\varepsilon)} \mathcal{U}'(\varepsilon)_{z(\varepsilon)}.$$

The set of points represented by  $\mathcal{U}(\varepsilon)'$  is  $\mathcal{A}(\varepsilon)$  (see (6.1)). Compute the limit of  $\mathcal{A}(\varepsilon)$  using Algorithm 3 (Limit of a Bounded Point).

- Step 2. Call Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets) with input  $\text{Def}(Q, \varepsilon)$  (cf. Notation 6.1), the triple  $(p, m, 0)$ , the real block representation  $\mathcal{F}, \sigma, [p^m], F$ , and  $\mathcal{U}'(\varepsilon)$  (note that since  $r = 0$  in the input there is no triangular Thom encoding  $H, \rho$  specified in the input to this call). The output of Algorithm 2 consists of a set of real univariate representations and curve segments over triangular Thom encodings. Each such curve segment,  $\gamma(\varepsilon) = (f_1, \sigma_1, f_2, \sigma_2, g, \tau, G)$ , is defined over some  $(t, z_\gamma(\varepsilon))$  with  $r_\gamma < p$  and  $z_\gamma(\varepsilon) \in \mathbb{R}\langle \varepsilon \rangle^{r_\gamma}$ , represented by a triangular system  $\mathcal{F}, \mathcal{H}_\gamma(\varepsilon)$ .
- Step 3. For each such curve segment  $\gamma(\varepsilon)$  over  $(t, z_\gamma(\varepsilon))$ , output in the previous step, call Algorithm 4 (Limit of a Curve) with input the triangular system  $\mathcal{F}, \mathcal{H}_\gamma(\varepsilon)$  and  $\gamma(\varepsilon)$ . Finally, project to  $\mathbb{R}^k$  by forgetting the last coordinate.

*Remark 6.4.* The role played by the set of points  $\mathcal{A}(\varepsilon)$  whose limit is computed by Algorithm 5 (Limit of Roadmaps of Special Low Dimensional Varieties), will become clear in the proof of correctness of Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) (see (7.2)).

**PROOF OF CORRECTNESS.** First note that it follows from Proposition 6.2 that  $\text{Def}(Q, \varepsilon)_F$  satisfies Property 5.1, and hence  $\mathcal{A}(\varepsilon)$  is a finite set of points. The correctness of the algorithm now follows from the correctness of Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets) and Algorithm 4 (Limit of Curve).  $\square$

**COMPLEXITY ANALYSIS.** The number of arithmetic operations performed in  $\text{D}[\varepsilon]$  in Step 1 is bounded by  $D^{O(m+p)} d^{O((m+p)k)}$  arithmetic operations in  $\text{D}[\varepsilon]$  according to the complexity analysis of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] and [2, Algorithm 12.20 (Triangular Thom Encoding)]. Since the degree in  $\varepsilon$  in the output of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] is  $d^{O(k)}$  and does not change during the pseudo-reduction, the number of arithmetic operations in  $\text{D}$  in Step 1 and hence the complexity is bounded by  $D^{O(m+p)} d^{O((m+p)k)}$ .

The number of arithmetic operations performed in  $\text{D}[\varepsilon]$  in Step 2 is bounded by  $D^{O(m+p)} d^{O((m+p)k)}$  according to the complexity analysis of Algorithm 2 (Roadmap for Lower Dimensional Special Algebraic Sets). Moreover the degree in  $\varepsilon$  is bounded by  $O(d)^k$ . To see this one has to observe that the arithmetic operations in  $\text{D}[\varepsilon]$  in the call to Algorithm 1 (Curve Segments) coincide with those performed by [2, Algorithm 15.10 (Parametrized Curve Segments)] with  $\varepsilon$  treated as a parameter.

It follows from the complexity analysis of [2, Algorithm 15.10 (Parametrized Curve Segments)] that the degree in  $\varepsilon$  is bounded by  $O(d)^k$ .

So the number of arithmetic operations in D in Step 2 and hence the complexity is bounded by  $D^{O(m+p)} d^{O((m+p)k)}$ .

The complexity of Step 3 is also bounded by  $D^{O(m+p)} d^{O((m+p)k)}$  according to the complexity analysis of Algorithm 4 (Limit of Curve).

Thus the total complexity of the algorithm is  $D^{O(m+p)} d^{O((m+p)k)}$ .  $\square$

## 7. MAIN RESULT

We now describe our main result Algorithm 7 (Baby-giant Roadmap for General Algebraic Sets). It is based on Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets), computing a baby step - giant step roadmap algorithm for a bounded algebraic set. The algorithm for computing roadmaps of general (i.e. not necessarily bounded) algebraic sets, Algorithm 7 (Baby-giant Roadmap for General Algebraic Sets) is then obtained from Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) following a method similar to the one in [2] to go from the bounded case to the general case.

Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) proceeds roughly as follows. We denote by  $y$  the vector of coordinates which are fixed. If the number of non-fixed coordinates is too small (i.e. less than the number  $p$  which is prescribed in the input), then we compute the roadmap using [2, Algorithm 15.3 (Bounded Algebraic Roadmap)]. Otherwise, we compute representations of points in  $\mathcal{N}_y \subset \mathbb{R}^p$  defining the fibers at which we make recursive calls to the same algorithm; these are the giant steps.

For the baby steps, the algorithm uses Algorithm 5 (Limit of Roadmaps of Special Low Dimensional Varieties) to compute the limit (under the  $\lim_\varepsilon$  map) of the roadmap of the critical set  $W_{y,\varepsilon}^{(p)}$  going through a well chosen finite set of points.

We are now ready to proceed to the description of Algorithm 6.

We first introduce some notation to be used in the description of Algorithm 6 and the proof of its correctness.

**Notation 7.1.** The input of the algorithm involves

- (1) a polynomial  $Q \in \mathbb{D}[X_1, \dots, X_k]$  such that  $V = \text{Zer}(Q, \mathbb{R}^k) \subset \mathcal{B}_k(0, 1/c)$  (where  $c \in \mathbb{R}$ );
- (2)  $y \in \mathbb{R}^{mp}$
- (3) a finite set of points  $\mathcal{M}_0 \subset V_y = \text{Zer}(Q(y, -), \mathbb{R}^{k-mp})$ .

Let as in Notation 6.1

$$\begin{aligned} V(\varepsilon)_y &= \text{Zer}(\text{Def}(Q, \varepsilon)(y, -), \mathbb{R}\langle \varepsilon \rangle^{k-pm+1}), \\ W(\varepsilon)_y^{(p)} &= \text{Zer}(\text{Cr}_{\ell+p}(Q, \varepsilon)(y, -), \mathbb{R}\langle \varepsilon \rangle^{k-pm+1}), \end{aligned}$$

and define

- (1)  $\mathcal{M}(\varepsilon) = W(\varepsilon)_y^{(0)} \subset V(\varepsilon)_y$ ;
- (2)  $\mathcal{D}(\varepsilon)^{(p)} \subset \mathbb{R}\langle \varepsilon \rangle$  the set of pseudo-critical values (see [2, Definition 12.41]) of  $\pi_{\ell+1}$  on  $W(\varepsilon)_y^{(p)}$  and  $\mathcal{M}(\varepsilon)^{(p)}$  a set of points such that for every  $c \in \mathcal{D}(\varepsilon)^{(p)}$ ,  $\mathcal{M}(\varepsilon)^{(p)}$  intersects every s-a connected component  $D$  of  $(W(\varepsilon)_y^{(p)})_c$ .

It follows from Proposition 6.2 and Proposition 5.3 that

$$\left( V(\varepsilon)_y, \mathcal{M}(\varepsilon), W(\varepsilon)_y^{(p)}, \mathcal{M}(\varepsilon)^{(p)}, \mathcal{D}(\varepsilon)^{(p)} \right)$$

satisfies Property 3.2.

We also define

$$\begin{aligned}
\mathcal{N}(\varepsilon) &= \pi_{[mp+1, (m+1)p]}(\mathcal{M}(\varepsilon)), \\
\mathcal{N} &= \lim_{\varepsilon}(\mathcal{N}(\varepsilon)), \\
\mathcal{N}(\varepsilon)^{(p)} &= \pi_{[mp+1, (m+1)p]}(\mathcal{M}(\varepsilon)^{(p)}), \\
\mathcal{N}^{(p)} &= \lim_{\varepsilon}(\mathcal{N}(\varepsilon)^{(p)}), \\
\mathcal{N}_0 &= \pi_{[mp+1, (m+1)p]}(\mathcal{M}_0), \\
\mathcal{N}' &= \mathcal{N}_0 \cup \mathcal{N} \cup \mathcal{N}^{(p)}, \\
\mathcal{N}'(\varepsilon) &= \mathcal{N}_0 \cup \mathcal{N}(\varepsilon) \cup \mathcal{N}(\varepsilon)^{(p)}.
\end{aligned}$$

**ALGORITHM 6. [Baby-giant Roadmap for Bounded Algebraic Sets]**

- INPUT. (1) a polynomial  $Q \in \mathbb{D}[X_1, \dots, X_k]$  such that  $V = \text{Zer}(Q, \mathbb{R}^k) \subset \mathcal{B}_k(0, 1/c)$  (where  $c \in \mathbb{R}$ );  
(2)  $y \in \mathbb{R}^{mp}$  represented by a real block representation

$$\mathcal{F}, \sigma, [p^m], F,$$

(see (4.1)) such that  $t \in \mathbb{R}^m$  is represented by a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$ ;

- (3) a finite set of points  $\mathcal{M}_0$  in  $V_y = \text{Zer}(Q(y, -), \mathbb{R}^{k-mp})$  represented by quasi-monic real univariate representations  $\mathcal{U}_0$  over  $t$ . All the coefficients of the input polynomials are in  $\mathbb{D}$ .

OUTPUT. a representation of a roadmap,  $\text{BGRM}(V_y, \mathcal{M}_0)$ , for  $(V_y, \mathcal{M}_0)$ .

COMPLEXITY.  $d^{O(k^2/p+pk)}$  operations in  $\mathbb{D}$  where  $d = \deg(Q) \geq 2$  and the degrees of the polynomials in  $\mathcal{F}, F$ , as well as the degrees of the polynomials and the number of elements in  $\mathcal{U}_0$  are all bounded by  $d^{O(k)}$ .

PROCEDURE.

Step 1. If  $(m+1)p \geq k$  call [2, Algorithm 15.3 (Bounded Algebraic Roadmap)] with input

- (1) the quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$  representing  $t \in \mathbb{R}^m$ ,
- (2) the polynomial  $Q_F$ , using Notation 4.5,
- (3) the finite set of points  $\mathcal{M}_0$  in  $V_y = \text{Zer}(Q_F(t, -), \mathbb{R}^{k-mp})$  represented by real univariate representations  $\mathcal{U}_0$  over  $t$ .

Otherwise, do the following.

Step 2. Determine the finite set of points  $\mathcal{N}$ , and their representation  $\mathcal{U}$  used in the recursive call as follows.

Let  $T = (T_1, \dots, T_m)$ , and using Notation 4.5 and 6.1),

$$P = \sum_{A \in \text{Cr}_{(m+1)p}(Q, \varepsilon)_F} A^2 \in \mathbb{D}[\varepsilon, T, X_{mp+1}, \dots, X_k].$$

Step 2 a). Call [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] with input  $P$  and parameters  $\varepsilon, T$ , and output a set of parametrized univariate representations with variable  $U$ . Compute a pseudo-reduction of the output modulo  $\mathcal{F}$  (using Proposition 8.4) and place the result in  $\mathcal{U}(\varepsilon)$ .

For every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{U}(\varepsilon)$ , use [2, Algorithm 12.20 (Triangular Thom Encoding)] with input the triangular system  $(\mathcal{F}, h(\varepsilon))$  to compute the Thom

encodings of the real roots of  $h(\varepsilon)(y, U)$ . Let  $\mathcal{U}'(\varepsilon)$  be the set of real univariate representations over  $y$  so obtained. Let  $\mathcal{M}(\varepsilon) \subset V(\varepsilon)_y$  be the set of points represented by  $\mathcal{U}'(\varepsilon)$ .

Projecting  $\mathcal{U}'(\varepsilon)$ , by forgetting its components corresponding to the last  $k - (m + 1)p$  coordinates obtain a set of quasi-monic real univariate representations  $\mathcal{V}(\varepsilon)$  representing  $\mathcal{N}(\varepsilon)$  over  $t$ . Then apply Algorithm 3 (Limit of a Bounded Point) with  $\mathcal{V}(\varepsilon)_y$  as input to obtain a set of quasi-monic real univariate representations  $\mathcal{V}$  representing  $\mathcal{N}$  over  $t$ .

Step 2 b). Perform Algorithm 1 (Curve Segment) with input  $P$  and the triangular Thom encoding  $\mathcal{F}, \sigma$  and retain the set of univariate representations,  $\mathcal{U}(\varepsilon)^{(p)}$ , representing  $\mathcal{M}(\varepsilon)^{(p)} \subset V(\varepsilon)_y$ , which are the distinguished points in the output.

Projecting  $\mathcal{U}(\varepsilon)^{(p)}$ , by forgetting its components corresponding to the last  $k - (m + 1)p$  coordinates obtain a set of real univariate representations  $\mathcal{V}(\varepsilon)^{(p)}$  representing  $\mathcal{N}(\varepsilon)^{(p)}$ . Then apply Algorithm 3 (Limit of a Bounded Point) with  $\mathcal{V}(\varepsilon)_y^{(p)}$  as input to obtain a set of quasi-monic real univariate representations  $\mathcal{V}^{(p)}$  representing  $\mathcal{N}^{(p)}$ .

Step 2 c). Projecting  $\mathcal{U}_0$ , by its components corresponding to the last  $k - (m + 1)p$  coordinates obtain a set of quasi-monic real univariate representations  $\mathcal{V}_0$  representing  $\mathcal{N}_0$  over  $t$ .

Let

$$\mathcal{V}' = \mathcal{V}_0 \cup \mathcal{V} \cup \mathcal{V}^{(p)},$$

and

$$\mathcal{V}'(\varepsilon) = \mathcal{V}_0 \cup \mathcal{V}(\varepsilon) \cup \mathcal{V}(\varepsilon)^{(p)}.$$

Step 3. Call Algorithm 5 (Limit of Roadmaps of Special Low Dimensional Varieties) with input  $p, Q$ , the real block representation  $\mathcal{F}, \sigma, [p^m], F$ , and  $\mathcal{V}'(\varepsilon)_y$  and note that the one-dimensional s-a set described by the output contains the image under the  $(\pi_{[1,k]} \circ \lim_\varepsilon)$  map of the finite set

$$\mathcal{A}(\varepsilon) = \bigcup_{z(\varepsilon) \in \mathcal{N}'(\varepsilon)} W(\varepsilon)_{y, z(\varepsilon)}^{(0)}.$$

Place the result in the output.

Recursive call. For every element  $u = ((\mathcal{F}, h), (\sigma, \tau), (F, H)) \in \mathcal{V}'$ , representing  $(y, z) \in \mathcal{N}' \subset \mathbb{R}^{(m+1)p}$ , determine a set,  $\mathcal{U}_z$ , of quasi-monic univariate representations over  $u$  representing

$$\mathcal{M}_z = (\pi_{[1,k]} \circ \lim_\varepsilon) \left( \bigcup_{z(\varepsilon) \in \mathcal{N}'(\varepsilon), \lim_\varepsilon(z(\varepsilon)) = z} W(\varepsilon)_{y, z(\varepsilon)}^{(0)} \right) \quad (7.1)$$

using Algorithm 3 (Limit of a Bounded Point).

Call Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) recursively with input

$$Q, (\mathcal{F}, h), (\sigma, \tau), [p^{m+1}], (F, H),$$

and  $\mathcal{U}_z \cup (\mathcal{U}_0)_z$ , where  $(\mathcal{U}_0)_z$  is a set of quasi-monic real univariate representations representing  $(\mathcal{M}_0)_z$ .

*Remark 7.2.* Algorithm 6 would have been much simpler if we could make recursive calls to Algorithm 6 at the fibers over the points in  $\mathcal{N}_\varepsilon$ , and thus obtain a roadmap first of  $V(\varepsilon)_y$ , and finally take the image of the resulting roadmap under the  $\lim_\varepsilon$  map. In this case the proof of correctness of the algorithm would be an immediate consequence of the main connectivity result, Corollary 5.3, and the fact that the image under  $\lim_\varepsilon$  of a bounded, s-a connected set is also s-a connected.

However, we are unable to compute efficiently limits of s-a curves given by curve segments over a real block representation which depend on  $\varepsilon$ , if the number of blocks and their sizes are large. More precisely, if the number of blocks as well as the sizes of the blocks are proportional to  $\sqrt{k}$ , then the procedure that we use to compute limits of curve segments could produce polynomials with degrees as large as  $d^{ck^2}$  in  $\varepsilon$  where  $c$  is some constant  $> 0$ . This is unacceptable since we are aiming for a roadmap algorithm having complexity  $d^{O(k\sqrt{k})}$ .

We overcome this difficulty by making recursive calls to Algorithm 6, not at the fibers over the points in  $\mathcal{N}(\varepsilon)$ , but at the fibers over  $\mathcal{N} = \lim_\varepsilon(\mathcal{N}(\varepsilon))$ , so that the algebraic sets specified in the input to the various recursive calls are then  $V_{(y,z)}$  for  $z \in \mathcal{N}$ . In this approach, the only limits of curve segments that are computed are those of the roadmap of  $W(\varepsilon)_y^{(p)}$ , and we can compute the limits of these curve segments without spoiling the complexity, as they are not defined over real block representations depending on  $\varepsilon$ . However, since the recursive calls are made with fibers of  $V_y$  (instead of  $V(\varepsilon)_y$ ), Corollary 5.3 is not directly applicable, and we need to be more careful about choosing the set of points in the input to the recursive calls. It also makes the proof of correctness more complicated.

#### PROOF OF CORRECTNESS.

##### Base case.

If  $\lceil (k - mp)/p \rceil = 1$  then the correctness of the algorithm is a consequence of the correctness of [2, Algorithm 15.3 (Bounded Algebraic Roadmap)].

##### General case.

Suppose that  $\lceil (k - mp)/p \rceil > 1$ .

Denote by  $\text{BGRM}(V_y, \mathcal{M}_0)$  the union of the curve segments output by Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets).

We have that

$$\text{BGRM}(V_y, \mathcal{M}_0) = \mathcal{R} \cup \bigcup_{(y,z) \in \mathcal{N}'} \text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z),$$

with

$$\mathcal{R} = (\pi_{[1,k]} \circ \lim_\varepsilon)(\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))),$$

denoting as before by  $W(\varepsilon)_y^{(p)}$  the zero set of  $\text{Cr}_{(m+1)p}(Q, \varepsilon)_F$  and

$$\mathcal{A}(\varepsilon) = \bigcup_{z(\varepsilon) \in \mathcal{N}'(\varepsilon)} W(\varepsilon)_{y,z(\varepsilon)}^{(0)}$$

(see Notation 7.1).

**Proof of  $\mathcal{M}_0 \subset \text{BGRM}(V_y, \mathcal{M}_0)$ .**

The proof is by induction on  $\lceil (k - mp)/p \rceil$ .

We suppose by induction that for every  $(y, z) \in \mathcal{N}$

$$\mathcal{M}_z \cup (\mathcal{M}_0)_z \subset \text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z).$$

Since  $\mathcal{M}_0 \subset \bigcup_{(y,z) \in \mathcal{N}} (\mathcal{M}_0)_z$ , and by induction hypothesis we have that

$$(\mathcal{M}_0)_z \subset \text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z),$$

it is clear that  $\text{BGRM}(V_y, \mathcal{M}_0)$  contains  $\mathcal{M}_0$ .

**Proof of RM<sub>1</sub>.**

The property RM<sub>1</sub> of  $\text{BGRM}(V_y, \mathcal{M}_0)$  is also proved by induction on  $\lceil (k - mp)/p \rceil$ .

Let  $C$  be a s-a connected component of  $V_y$ , and  $C' = \text{BGRM}(V_y, \mathcal{M}_0) \cap C$ . We want to prove that  $C'$  is s-a connected.

Supposing that  $x, x' \in C'$ , we are going to prove that there exists a s-a path  $\gamma : [0, 1] \rightarrow C'$  with  $\gamma(0) = x, \gamma(1) = x'$ .

**Without loss of generality we can suppose that  $x \in \mathcal{R}$ :**

Since

$$\text{BGRM}(V_y, \mathcal{M}_0) = \mathcal{R} \cup \bigcup_{(y,z) \in \mathcal{N}'} \text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z),$$

we have that  $x$  (resp.  $x'$ ) belongs to  $\mathcal{R}$  or to some  $\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  with  $(y, z) \in \mathcal{N}'$ .

If  $x \in \text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  we show that  $x$  can be connected to a point in  $\mathcal{M}_z$  inside

$$\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$$

by a s-a path. It follows from Proposition 5.3 that  $\text{Def}(Q, \varepsilon)_F$  satisfies Property 3.2 (2), and hence we have that  $W(\varepsilon)_{(y,z)}^{(0)}$  meets every s-a connected component of  $V(\varepsilon)_{(y,z)}$ . By [3, Lemma 15.6] each s-a connected component of  $V_{(y,z)}$  is the image under  $\pi_{[1,k]} \circ \lim_\varepsilon$  of a unique s-a connected component of  $V(\varepsilon)_{(y,z)}$ . It follows that each s-a connected component of  $V_{(y,z)}$  meets

$$\pi_{[1,k]} \circ \lim_\varepsilon (W(\varepsilon)_{(y,z)}^{(0)}) \subset \mathcal{M}_z,$$

since

$$W(\varepsilon)_{(y,z)}^{(0)} = (W(\varepsilon)_y^{(p)})_z.$$

Finally, applying the induction hypothesis to  $\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  we have that the intersection of  $\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  with each s-a connected component of  $V_{(y,z)}$  is non-empty and s-a connected, and meets  $\mathcal{M}_z$ . Thus, there exists a s-a path in  $\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  joining  $x$  to a point in  $\mathcal{M}_z$ .

Since  $\mathcal{M}_z \subset \mathcal{R}$  we can assume that  $x$  (and similarly  $x'$ ) is contained in  $\mathcal{R}$ .

**Connectivity when  $x$  and  $x'$  are contained in  $\mathcal{R}$ .**

Since

$$\mathcal{R} = (\pi_{[1,k]} \circ \lim_\varepsilon)(\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))),$$

there exists  $x(\varepsilon) \in \text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$  (resp.  $x'(\varepsilon) \in \text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$ ) such that  $\lim_\varepsilon(x(\varepsilon)) = x$  (resp.  $\lim_\varepsilon(x'(\varepsilon)) = x'$ ).

Let

$$\mathcal{S}(\varepsilon) = W(\varepsilon)_y^{(p)} \cup (V(\varepsilon)_y)_{\mathcal{N}'(\varepsilon)},$$

and  $C(\varepsilon)$  the unique s-a connected component of  $V(\varepsilon)_y$  such that  $(\pi_{[1,k]} \circ \lim_\varepsilon)(C(\varepsilon)) = C$ .

By Corollary 3.9, since  $\mathcal{N}(\varepsilon) \cup \mathcal{N}(\varepsilon)^{(p)} \subset \mathcal{N}'(\varepsilon)$ ,  $\mathcal{S}(\varepsilon) \cap C(\varepsilon)$  is s-a connected. So there exists a s-a path  $\gamma(\varepsilon) : [0, 1] \rightarrow \mathcal{S}(\varepsilon) \cap C(\varepsilon)$ , with  $\gamma(\varepsilon)(0) = x(\varepsilon), \gamma(\varepsilon)(1) =$

$x'(\varepsilon)$ . Moreover, there exists a partition of  $(0, 1) \subset \mathbb{R}\langle\varepsilon\rangle$  into a finite number of open intervals and points, such that for every open interval  $I$  in the partition one of the following holds :

Case 1:

$$\gamma(\varepsilon)(I) \subset W(\varepsilon)_y^{(p)}.$$

Case 2: there exists  $z(\varepsilon) \in \mathcal{N}'(\varepsilon)$  such that

$$\gamma(\varepsilon)(I) \subset V(\varepsilon)_{(y, z(\varepsilon))}.$$

Since  $W(\varepsilon)_y^{(p)} \subset V(\varepsilon)_y$ , for each point  $a \in (0, 1)$  defining the partition

$$\gamma(\varepsilon)(a) \in \mathcal{A}(\varepsilon) \subset \text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon)). \quad (7.2)$$

Hence, by definition of  $\mathcal{M}_z$  (see (7.1))

$$(\pi_{[1, k]} \circ \lim_{\varepsilon})(\gamma(\varepsilon)(a)) \in \mathcal{M}_z, \quad (7.3)$$

where  $\lim_{\varepsilon}(z(\varepsilon)) = z$ .

In Case 1, we can replace  $\gamma(\varepsilon)(I)$  by a s-a path having the same endpoints and whose image is contained in

$$\text{RM}(W(\varepsilon)_y^{(p)}, W_{\mathcal{N}'(\varepsilon)})$$

using  $\text{RM}_1$  as well as (7.2). Taking the image under  $\pi_{[1, k]} \circ \lim_{\varepsilon}$  of this new path we obtain a s-a path

$$\gamma : \lim_{\varepsilon}(I) \rightarrow \mathcal{R}.$$

In Case 2, writing  $I = (a, b)$ ,  $(\pi_{[1, k]} \circ \lim_{\varepsilon})(\gamma(\varepsilon)(a))$ ,  $(\pi_{[1, k]} \circ \lim_{\varepsilon})(\gamma(\varepsilon)(b))$  both belong to

$$\text{BGRM}(V_{(y, z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$$

using (7.3). Using the induction hypothesis for  $\text{BGRM}(V_{(y, z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)$  there exists a s-a path

$$\gamma : [\lim_{\varepsilon}(a), \lim_{\varepsilon}(b)] \rightarrow \text{BGRM}(V_{(y, z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z).$$

Finally, we have constructed a s-a path  $\gamma : [0, 1] \rightarrow C'$  with  $\gamma(0) = x$ ,  $\gamma(1) = x'$ .

This proves that  $\text{BGRM}(V_{(y, z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z) \cap C$  is non-empty and s-a connected proving  $\text{RM}_1$ .

**Proof of  $\text{RM}_2$ .**

Let  $c \in \mathbb{R}$  such that  $V_{(y, c)}$  is not empty, and let  $C$  be a s-a connected component of  $V_{(y, c)}$ . We prove that

$$\text{BGRM}(V_{(y, z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z) \cap C$$

is not empty. It follows from [3, Lemma 15.6] that there exists a s-a connected component  $C(\varepsilon)$  of  $V(\varepsilon)_{(y, c)}$  such that

$$C = (\pi_{[1, k]} \circ \lim_{\varepsilon})(C(\varepsilon)).$$

Since  $C(\varepsilon)$  is non-empty, let  $x(\varepsilon) \in C(\varepsilon)$  and let  $z(\varepsilon) = \pi_{[mp+1, (m+1)p]}(x(\varepsilon))$ . It follows from Proposition 5.3 that  $(W(\varepsilon)_y^{(p)})_{z(\varepsilon)} = W(\varepsilon)_{(y, z(\varepsilon))}^{(0)}$  meets every s-a connected component of  $V(\varepsilon)_{(y, z(\varepsilon))}$ . Since  $C(\varepsilon)$  contains a s-a connected component of  $V(\varepsilon)_{(y, z(\varepsilon))}$ , we have that

$$W(\varepsilon)_{(y, z(\varepsilon))}^{(0)} \cap C(\varepsilon) \neq \emptyset,$$



and thus  $C(\varepsilon)$  contains a s-a connected component of  $(W(\varepsilon)_y^{(p)})_c$  (since  $W(\varepsilon)_y^{(p)} \subset V(\varepsilon)_y$ ). Now, since the roadmap

$$\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$$

satisfies  $\text{RM}_2$ ,  $\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon))$  has a non-empty intersection with every s-a connected component of  $(W(\varepsilon)_y^{(p)})_c$ , and in particular with the one contained in  $C(\varepsilon)$ . Taking the image under the map  $(\pi_{[1,k]} \circ \lim_\varepsilon)$ , we get that  $\mathcal{R} = (\pi_{[1,k]} \circ \lim_\varepsilon)(\text{RM}(W(\varepsilon)_y^{(p)}, \mathcal{A}(\varepsilon)))$  has a non-empty intersection with  $(\pi_{[1,k]} \circ \lim_\varepsilon)(C(\varepsilon)) = C$ . Since  $\text{BGRM}(V_{(y,z)}, \mathcal{M}_z \cup (\mathcal{M}_0)_z)_c$  contains  $\mathcal{R}$ , this finishes the proof.  $\square$

**COMPLEXITY ANALYSIS.** We first bound the number of arithmetic operations in Step 1. Since we assume that the degrees of the polynomials in  $\mathcal{F}, F$  are bounded by  $d^{O(k)}$ , it follows from the complexity analysis of [2, Algorithm 15.3 (Bounded Algebraic Roadmap)], and [3, Algorithm 15.2 (Curve Segments)], that the number of arithmetic operations in this step is bounded by

$$d^{O(km)} d^{O((k-mp)^2)} = d^{O(km+mp^2)}$$

since  $k - mp \leq p$ .

The number of arithmetic operations in  $D[\varepsilon]$  in Step 2 is bounded by  $d^{O(mk)}$  and the degree and number of univariate representations produced is bounded by  $O(d)^{k-mp}$ . Moreover the degree in  $\varepsilon$  is bounded by  $O(d)^k$ . To see this one has to observe that the arithmetic operations in  $D[\varepsilon]$  in the call to Algorithm 1 (Curve Segments) coincide with those performed in [2, Algorithm 15.10 (Parametrized Curve Segments)] with  $\varepsilon$  treated as a parameter. It follows from the complexity analysis of [2, Algorithm 15.10 (Parametrized Curve Segments)] that the degree in  $\varepsilon$  is bounded by  $O(d)^k$ . So the number of arithmetic operations in  $D$  in Step 2 is bounded by  $d^{O(mk)}$ .

The complexity of computing  $\mathcal{R}_y$  in Step 3 is bounded by  $d^{O((m+p)k)}$  given that the number of arithmetic operations of Algorithm 5 (Limit of Roadmaps of Special Low Dimensional Varieties) is  $d^{O((m+p)k)}$ .

The total number of recursive calls at depth  $i$  is  $d^{O(ki)}$ , and for each such call the number of arithmetic operations in  $D$  in Steps 1, 2, and 3 is bounded by  $d^{O((m+i+p)k+p^2)}$ , where  $0 \leq i \leq \lfloor k/p \rfloor - m$ . Since the depth of the recursion is at most  $\lfloor k/p \rfloor - m$ , we conclude that the total number of arithmetic operations in the domain  $D$  is bounded by

$$d^{O(k^2/p)} d^{O((k/p+p)k+p^2)} = d^{O(k^2/p+pk)}.$$

$\square$

We now describe Algorithm 7 (Baby-giant Roadmap for General Algebraic Sets) for computing a roadmap of a general (i.e. not necessarily bounded algebraic set). This algorithm is essentially the same algorithm as [2, Algorithm 15.5 (Algebraic Roadmap)], except that we call Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) after reducing to the bounded case instead of [2, Algorithm 15.3 (Bounded Algebraic Roadmap)]. We first need a notation. Let  $P \in \mathbb{R}[X]$  be given by

$$P = a_p X^p + \cdots + a_q X^q, \quad p > q, \quad a_q a_p \neq 0.$$

**Notation 7.3.** We write

$$c(P) = \left( \sum_{q \leq i \leq p} \left| \frac{a_i}{a_q} \right| \right)^{-1}.$$

**ALGORITHM 7. [Baby-giant Roadmap for General Algebraic Sets]**

**INPUT.** (1) a polynomial  $Q \in \mathbb{D}[X_1, \dots, X_k]$ ;  
 (2) a finite set of points  $\mathcal{M}_0$  in  $\text{Zer}(Q, \mathbb{R}^k)$ , represented by real univariate representations  $\mathcal{U}_0$ .

**OUTPUT.** a roadmap,  $\text{BGRM}(\text{Zer}(Q, \mathbb{R}^k), \mathcal{M}_0)$ , for  $(\text{Zer}(Q, \mathbb{R}^k), \mathcal{M}_0)$ .

**COMPLEXITY.**  $d^{O(k^2/p+pk)}$  operations in  $\mathbb{D}$ .

**PROCEDURE.**

Step 1. Introduce new variables  $X_{k+1}$  and  $\varepsilon$  and replace  $Q$  by the polynomial

$$Q(\varepsilon) = Q^2 + (\varepsilon^2(X_1^2 + \dots + X_{k+1}^2) - 1)^2.$$

Replace  $\mathcal{M}_0 \subset \mathbb{R}^k$  by the set of real univariate representations representing the elements of  $\text{Zer}(\varepsilon^2(X_1^2 + \dots + X_{k+1}^2) - 1, \mathbb{R}\langle \varepsilon \rangle^{k+1})$  above the points  $\mathcal{M}_0$  using [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)].

Step 2. Call Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets) with input  $Q(\varepsilon)$ ,  $\mathcal{M}_0$ ,  $m = 0$ , performing arithmetic operations in the domain  $\mathbb{D}[\varepsilon]$ . The algorithm outputs a roadmap

$$\text{BGRM}(\text{Zer}(Q(\varepsilon), \mathbb{R}\langle \varepsilon \rangle^{k+1}), \mathcal{M}_0)$$

composed of points and curves whose description involves  $\varepsilon$ .

Step 3. Denote by  $\mathcal{L}$  the set of polynomials in  $\mathbb{D}[\varepsilon]$  whose signs have been determined in the preceding computation and take

$$a = \min_{P \in \mathcal{L}} c(P)$$

(Notation 7.3). Replace  $\varepsilon$  by  $a$  in the polynomial  $Q(\varepsilon)$  to get a polynomial  $Q_a$ . Replace  $\varepsilon$  by  $a$  in the output roadmap to obtain a roadmap  $\text{BGRM}(\text{Zer}(Q_a, \mathbb{R}^{k+1}), \mathcal{M}_0)$ . When projected to  $\mathbb{R}^k$ , this roadmap gives a roadmap

$$\text{BGRM}(\text{Zer}(Q, \mathbb{R}^k), \mathcal{M}_0) \cap \mathcal{B}_k(0, 1/a).$$

Step 4. In order to extend the roadmap outside the ball  $B(0, 1/a)$  collect all the points  $(y_1, \dots, y_k, y_{k+1}) \in \mathbb{R}\langle \varepsilon \rangle^{k+1}$  in the roadmap

$$\text{BGRM}(\text{Zer}(Q(\varepsilon), \mathbb{R}\langle \varepsilon \rangle^{k+1}), \mathcal{M}_0)$$

which satisfy  $\varepsilon(y_1^2 + \dots + y_k^2) = 1$ . Each such point is described by a real univariate representation involving  $\varepsilon$ . Add to the roadmap the curve segment obtained by first forgetting the last coordinate and then treating  $\varepsilon$  as a parameter which varies over  $(0, a]$  to get a roadmap  $\text{BGRM}(\text{Zer}(Q, \mathbb{R}^k), \mathcal{M}_0)$ .

**PROOF OF CORRECTNESS.** The proof of correctness follows from the proof of correctness of Algorithm 6 (Baby-giant Roadmap for Bounded Algebraic Sets).  $\square$

**COMPLEXITY ANALYSIS.** The complexity is dominated by the complexity of Step 2.  $\square$

*Proofs of Theorem 1.2 and Corollary 1.3.* Follows directly from the correctness and complexity analysis of Algorithm 7 (Baby-giant Roadmap for General Algebraic Sets), after substituting  $m = 0$  and  $p = \sqrt{k}$ .  $\square$

## 8. APPENDIX: COMPUTING THE LIMIT OF BOUNDED POINTS AND CURVE SEGMENTS

**8.1. Limit of a bounded point.** Before computing the limit of a bounded point we need to explain how to perform some useful computations modulo a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$  representing a point  $t \in \mathbb{R}^m$ .

We associate to  $t \in \mathbb{R}^m$  specified by a triangular Thom encoding  $\mathcal{F}, \sigma$ ,

$$\mathcal{F} = (f_{[1]}, \dots, f_{[m]}), f_{[i]} \in \mathbb{D}[T_1, \dots, T_i],$$

the ordered domain  $\mathbb{D}[t]$  contained in  $\mathbb{R}$  and generated by  $t$ .

We now aim at describing the pseudo-inversion of a non-zero element in the domain  $\mathbb{D}[t]$  specified by  $\mathcal{F}, \sigma$ .

**Definition 8.1.** A pseudo-inverse of  $f \in \mathbb{D}[t]$  is an element  $g \in \mathbb{D}[t]$  such that  $fg \in \mathbb{D}$  is strictly positive.

This notion is delicate as the computation of the pseudo-inverse sometimes requires us to update the quasi-monic triangular Thom encoding specifying  $t$ , in the spirit of dynamical methods in algebra (see for example [7]). We start with a motivating example.

**Example 8.2.** We consider  $t$ , specified as the root of

$$f(T) = T^4 - T^2 - 2$$

giving signs  $(+, +, +, +)$  to the set  $\text{Der}(f)$  of derivatives of  $f$ .

Consider  $T^2 + 1$ . It is easy to see, using for example [2, Algorithm 10.13 (Sign Determination Algorithm)] applied to  $f$  and the list  $\text{Der}(f), T^2 + 1$ , that the sign of  $T^2 + 1$  at  $t$  is positive. In order to compute its pseudo-inverse, we perform [2, Algorithm 8.22 (Extended Signed Subresultant)] of  $f$  and  $T^2 + 1$ . If  $f(T)$  and  $T^2 + 1$  were coprime, we would obtain the pseudo-inverse of  $T^2 + 1$  modulo  $f(T)$  since the last subresultant would be a non-zero constant in  $\mathbb{D}$ . But  $f(T)$  and  $T^2 + 1$  are not coprime and their gcd is  $T^2 + 1$ . So we divide  $f(T)$  by  $T^2 + 1$ , obtain a new polynomial  $g(T) = T^2 - 2$  and check that the root  $t$  of  $f(T)$  giving signs  $(+, +, +, +)$  to the set  $\text{Der}(f)$  coincides with  $\sqrt{2}$  which is the root of  $T^2 - 2$  making the derivative  $g'(T) = 2T$  positive, using again -for example- [2, Algorithm 10.13 (Sign Determination Algorithm)]. It is now possible to compute a pseudo-reduction of  $T^2 + 1$  modulo  $g(T)$ , which gives 3.

In other words, during the process of computing the pseudo-inverse of  $T^2 + 1$  we discovered the factor  $g(T)$  of  $f(T)$  having  $t$  as a root and coprime with  $T^2 + 1$ . Using this new description of  $t$  we have been able to compute a pseudo-inverse of  $T^2 + 1$ .

We can now describe the computation of the pseudo-inverse in general.

**Description 8.3.** Given  $t = (t_1, \dots, t_m) \in \mathbb{R}^m$  specified by the quasi-monic triangular Thom encoding  $\mathcal{F} = (f_{[1]}, \dots, f_{[m]}), \sigma = (\sigma_1, \dots, \sigma_m)$ , we describe how to compute a pseudo-inverse of a non-zero element of  $\mathbb{D}[t]$ .

We proceed by induction on the number  $m$  of variables of  $\mathcal{F}$ .

If  $m = 0$ , there is nothing to do since  $D$  is an ordered domain.

If  $m \neq 0$ , let  $t' = (t_1, \dots, t_{m-1})$  specified by  $\mathcal{F}' = (f_{[1]}, \dots, f_{[m-1]}), \sigma = (\sigma_1, \dots, \sigma_{m-1})$ .

We consider  $f$  as a polynomial in  $T_m$  whose coefficients, which are elements of

$$\{h \in D[T_1, \dots, T_{m-1}] \mid \deg_{T_i}(h) < \deg_{T_i}(f_{[i]}), i = 1, \dots, m-1\},$$

represent elements of  $D[t']$ .

We first decide the sign of  $f$  at  $t$ , which is done by [2, Algorithm 12.19 (Triangular Sign Determination Algorithm)].

If  $f(t) \neq 0$ , we try to pseudo-invert  $f$  modulo  $\mathcal{F}$ . We perform [2, Algorithm 8.22 (Extended Signed Subresultant)] for  $f$  and  $f_{[m]}$ , with respect to the variable  $T_m$  and compute a  $\gcd(f, f_{[m]}) \in D[t']$  (the last non zero subresultant polynomial) as well as the cofactors  $u, v \in D[t']$  with  $uf + vf_{[m]} = \gcd(f, f_{[m]})$ .

- (1) If  $\gcd(f, f_{[m]})$  is of degree 0 in  $T_m$ ,  $u$  is a quasi-inverse of  $f$ .
- (2) If  $\gcd(f, f_{[m]})$  is of degree  $> 0$  in  $T_m$ , we have discovered a factor of  $f_{[m]}$ . We define  $h$  as the quasi-monic polynomial proportional to  $f_{[m]}/\gcd(f, f_{[m]})$  obtained by [2, Algorithm 8.22 (Extended Signed Subresultant)] (see [2, Algorithm 10.1 (Gcd and Gcd-free part)]). We perform [2, Algorithm 12.19 (Triangular Sign Determination)] applied to  $f_{[m]}$  and  $\text{Der}(f_{[m]}), \text{Der}(h)$  to identify the Thom encoding  $\tau$  of  $t_{[m]}$  as a root of  $h$ . We replace  $f_{[m]}$  by  $h$  and  $\sigma_{[m]}$  by  $\tau$  in  $\mathcal{F}$ . Now  $f$  and the new  $f_{[m]}$ , considered as polynomials in  $T_{[m]}$  are coprime, and we can invert  $f$  modulo  $f_{[m]}$ .

**Proposition 8.4.** *Let  $D$  be an ordered domain contained in a real closed field  $R$ , and  $t = (t_1, \dots, t_m) \in R^m$  be specified by a quasi-monic triangular Thom encoding  $\mathcal{F}, \sigma$ ,*

$$\mathcal{F} = (f_{[1]}, \dots, f_{[m]}), f_{[i]} \in D[T_1, \dots, T_i].$$

*Let  $d$  be a bound of the degree of  $f_{[i]}$  with respect to each  $T_j$ ,  $1 \leq j \leq i, 1 \leq i \leq m$ .*

*a) If  $g \in D[T_1, \dots, T_m]$  is a polynomial of degree  $D$ , the complexity of computing a pseudo-reduction  $(c, \bar{g})$  of  $g$  modulo  $\mathcal{F}$  is  $(Dd)^{O(m)}$  arithmetic operations in  $D$ .*

*b) The complexity of the computation of the pseudo-inverse of an element of  $D[t]$  is  $d^{O(m)}$  arithmetic operations in  $D$ .*

*Proof.* a) Suppose that  $C_g \in D$  is such that  $C_g T_1^{i_1} \dots T_m^{i_m} g$  has a reduction in  $D$  modulo  $\mathcal{F}$  for every  $(i_1, \dots, i_m)$  with  $i_j < \deg(f_{[j]}, T_j)$ ,  $1 \leq j \leq m$ . We denote by  $\text{Mat}(C_g g)$  the matrix of multiplication by  $C_g g$  modulo  $(\mathcal{F})$  with respect to monomial bases. The entries of  $\text{Mat}(C_g g)$  are in  $D$ . Its rows and columns are indexed by  $(i_1, \dots, i_m)$ ,  $i_j < \deg(f_{[j]}, T_j)$ ,  $1 \leq j \leq m$  and the  $(j_1, \dots, j_m)$ -th entry of the column indexed by  $(i_1, \dots, i_m)$  is the coefficient of  $T_1^{j_1} \dots T_m^{j_m}$  in the reduction of  $C_g T_1^{i_1} \dots T_m^{i_m} g$  modulo  $\mathcal{F}$ . Note that  $\text{Mat}(C_g C_h g h) = \text{Mat}(C_g g) \text{Mat}(C_h h)$ . Note also that the entries of the first column of  $\text{Mat}(C_g g)$  (indexed by  $(0, \dots, 0)$ ) are the coefficients of the reduction of  $C_g g$  modulo  $\mathcal{F}$ .

We first compute  $C_{T_j}$  such that  $C_{T_j} T_1^{i_1} \dots T_m^{i_m} T_j$  has a reduction in  $D$  modulo  $\mathcal{F}$  for every  $(i_1, \dots, i_m)$ ,  $i_h < \deg(f_{[h]}, T_h)$ ,  $1 \leq h \leq m$ . The algorithm proceeds by induction on  $j$ .

For  $j = 1$ , let  $c_1 \in D$  be the leading coefficient of  $f_{[1]} \in D[T_1]$ ,  $d_1 = \deg(f_{[1]}, T_1)$ , and  $C_{T_1} = c_1$ . The matrix  $\text{Mat}(c_1 T_1)$  is simply obtained by replacing each occurrence of  $c_1 T_1^{d_1}$  by  $f_{[1]} - c_1 T_1^{d_1}$  in

$$c_1 T_1^{d_1-1} T_2^{i_2} \dots T_m^{i_m} T_1$$

with  $i_h < d_h$ ,  $2 \leq h \leq m$  and writing the result as a linear combination of the monomials  $T_1^{j_1} \dots T_m^{j_m}$ ,  $j_i < d_i$ ,  $1 \leq i \leq m$ . Compute  $\text{Mat}(C_{T_1}^h T_1^h) = \text{Mat}(c_1 T_1)^h$ ,  $h < 2d$ , and define  $C_1 = c_1^{2d-1}$ .

Suppose by induction that for every monomial  $M$  in  $T_1, \dots, T_j$  of degree  $< 2d$ ,  $C_M T_1^{i_1} \dots T_m^{i_m} M$  has a reduction in  $D$  modulo  $\mathcal{F}$  for every  $(i_1, \dots, i_m)$ ,  $i_j < \deg(f_{[j]}, T_j)$ ,  $1 \leq j \leq m$ . Also, suppose that  $\text{Mat}(C_M M)$  has been computed. Denote by  $C_j \in D$  the product of  $C_M$  for all the monomials  $M$  of degree  $< 2d$  in the  $j$  variables  $T_1, \dots, T_j$ .

Let  $c_{j+1} \in D$  be the leading coefficient of  $f_{[j+1]} \in D[T_1, \dots, T_{j+1}]$  with respect to  $T_{j+1}$  and  $d_{j+1} = \deg(f_{[j+1]}, T_{j+1})$ , and take  $C_{T_{j+1}} = c_{j+1} C_j$ . The matrix  $\text{Mat}(C_{T_{j+1}} T_{j+1})$  is obtained by replacing each occurrence of  $C_{T_{j+1}} T_{j+1}^{d_{j+1}}$  by  $C_j f_{[j+1]} - C_{T_{j+1}} T_{j+1}^{d_{j+1}}$  in

$$C_{T_{j+1}} T_1^{i_1} \dots T_j^{i_j} T_{j+1}^{d_{j+1}-1} T_{j+2}^{i_{j+2}} \dots T_m^{i_m} T_{j+1},$$

with  $i_\ell < d_\ell$ .

Notice that the polynomials obtained this way have degrees at most  $2d$  in  $T_1, \dots, T_j$ , and degrees  $< d_h$  in  $T_h$  for  $h > j$ . Reduce all such monomials using the matrices of multiplication computed before.

Finally compute for every monomial  $M$  of degree  $\leq D$  in  $T_1, \dots, T_m$ ,  $C_M$  and  $\text{Mat}(C_M M)$  by taking products of the  $C_{T_i}$  and the matrices  $\text{Mat}(C_{T_i} T_i)$  (respectively), and let  $C_g$  be the product of the  $C_M$  for all monomials  $M$  of degree  $\leq D$ . Now determine  $\text{Mat}(C_g g)$  by taking an appropriate linear combination of  $\text{Mat}(C_M M)$  and thus obtain the reduction of  $C_g g$  modulo  $\mathcal{F}$ .

Notice that the complexity of computing the  $C_{T_{j+1}}$ , and  $\text{Mat}(C_{T_{j+1}} T_{j+1})$  is bounded by  $d^{O(m)}$ . In the last step, there are  $O(D)^m$  monomials of degree at most  $D$ , and hence at most  $O(D)^m$  matrix multiplications to perform, and the sizes of the matrices is  $d_1 \dots d_m \leq d^m$ . So the complexity is  $(Dd)^{O(m)}$ .

b) The proof proceeds by induction on the number of variables  $m$  of  $\mathcal{F}$ .

If  $m = 1$ , the computation of a gcd takes  $(d+1)^c$  operations in the domain  $D$ , for some universal constant  $c > 0$ , using the complexity analysis of [2, Algorithm 8.22 (Extended Signed Subresultant)] and [2, Algorithm 10.13 (Sign Determination)].

If  $m > 1$ , let  $t = (t', u)$ , and we suppose by induction hypothesis that the complexity of arithmetic operations including pseudo-inversion in  $D[t']$  is  $(d+1)^{c(m-1)}$  arithmetic operations in the ordered domain  $D$ . The claim is clear since the arithmetic operations in the domain  $D[t]$  are using  $(d+1)^c$  operations in the domain  $D[t']$  using the complexity analysis of [2, Algorithm 8.22 (Extended Signed Subresultant)] and [2, Algorithm 10.13 (Sign Determination)].  $\square$

We can now give the description of Algorithm 3 (Limit of a Bounded Point).

### Description of Algorithm 3 (Limit of a Bounded Point)

The precise input and output of this algorithm appear in Section 6.2.

PROCEDURE Remove from  $g(\varepsilon)(T_1, \dots, T_m, U)$  the coefficients vanishing at the point  $(t_1, \dots, t_m)$ , using [2, Algorithm 12.19 (Triangular Sign Determination)].  
Supposing without loss of generality that not all the coefficients of

$$g(\varepsilon)(t_1, \dots, t_m, U)$$

are multiples of  $\varepsilon$ , denote by  $g(T_1, \dots, T_m, U)$  the polynomial obtained by substituting 0 for  $\varepsilon$  in  $g(\varepsilon)(T_1, \dots, T_m, U)$ .

Similarly denote by  $G(T_1, \dots, T_m, U)$  the polynomials obtained by substituting 0 for  $\varepsilon$  in  $G(\varepsilon)(T_1, \dots, T_m, U)$ .

Compute the set  $\Sigma$  of Thom encodings of roots of  $g(t, U)$  using [2, Algorithm 12.19 (Triangular Sign Determination)]. Denoting by  $\mu_\sigma$  the multiplicity of the root of  $g(t, U)$  with Thom encoding  $\sigma$ , define  $G_\sigma$  as the  $(\mu_\sigma - 1)$ -th derivative of  $G$  with respect to  $U$ .

Identify the Thom encoding  $\sigma$  and  $G_\sigma$  representing  $z$  using [2, Algorithm 12.19 (Triangular Sign Determination)], by checking whether a ball of infinitesimal radius  $\delta$  ( $1 \gg \delta \gg \varepsilon > 0$ ) around the point  $x$  represented by the real univariate representation  $g, \sigma, G_\sigma$  contains  $z(\varepsilon)$ .

Pseudo-invert the leading coefficient of the univariate representation, denote by  $\mathcal{F}', \sigma'$  the new triangular Thom encoding describing  $t$  and compute a pseudo-reduction of the output modulo  $\mathcal{F}'$ .

*Complexity analysis:* Follows from the complexity of [2, Algorithm 12.19 (Triangular Sign Determination)].  $\square$

**8.2. Limit of a curve.** Computing the limit of a curve is not immediate when some part of the curve has a vertical limit, as seen in the following example.

**Example 8.5.** Consider the s-a curve  $\gamma : [0, \varepsilon] \rightarrow \mathbb{R}\langle \varepsilon \rangle^3$ , parametrized by the  $X_1$  coordinate defined by

$$\gamma(x_1) = (x_1, \gamma_2(x_1), \gamma_3(x_1)), x_1 \in [0, \varepsilon]$$

where  $(\gamma_2(x_1), \gamma_3(x_1))$  is the solution of the triangular system,

$$\begin{aligned} X_2 - x_1/\varepsilon &= 0, \\ X_2^2 + X_3^2 - 1 &= 0, \end{aligned}$$

with Thom encoding  $(0, +), (0, +, +)$ .

Notice that the image of  $\gamma$  is contained in the cylinder of unit radius with axis the  $X_1$ -axis and is bounded over  $\mathbb{R}$ . The image of  $\gamma$  under the  $\lim_\varepsilon$  map is contained in a circle in the plane  $X_1 = 0$ , and can no longer be described as a curve parametrized by the  $X_1$ -coordinate.

However, it is possible to reparametrize  $\gamma$  by the  $X_2$ -coordinate. By doing so we obtain another s-a curve  $\varphi : [0, 1] \rightarrow \mathbb{R}\langle \varepsilon \rangle^3$  (having the same image as  $\gamma$ ) defined by

$$\varphi(x_2) = (\varphi_1(x_2), x_2, \varphi_3(x_2)), x_2 \in [0, 1]$$

where  $(\varphi_1(x_2), \varphi_3(x_2))$  is the real solution of the triangular system

$$\begin{aligned} X_1 - \varepsilon x_2 &= 0, \\ X_3^2 + x_2^2 - 1 &= 0, \end{aligned}$$

with Thom encoding  $(0, -), (0, +, +)$ . Notice that the image under  $\lim_\varepsilon$  of the curve which is the graph of  $\varphi$  can be easily described as the curve represented by the following triangular system parametrized by  $x_2 \in [0, 1]$

$$\begin{aligned} X_1 &= 0, \\ X_3^2 + x_2^2 - 1 &= 0, \end{aligned}$$

and Thom encoding  $(0, -1), (0, +, +)$ .

This is the reason why some kind of reparametrization is necessary before computing the limit.

**8.2.1. Reparametrization of curve segments.** We define the notion of well-parametrized curve, and prove that the limit of a well-parametrized curve is easy to describe.

**Definition 8.6.** A differentiable s-a curve

$$\gamma = (\gamma_1, \dots, \gamma_k) : (a, b) \rightarrow \mathbb{R}^k$$

parametrized by  $X_1$  (i.e.  $\gamma_1(x_1) = x_1$ ) is *well-parametrized* if for every  $x_1 \in (a, b)$ ,

$$\sum_{i=1}^k \left( \frac{\partial \gamma_i}{\partial X_1} \right)^2 \leq k.$$

Let  $t \in \mathbb{R}^m$  be represented by a triangular Thom encoding  $\mathcal{F}, \sigma$ , and

$$f_1, \sigma_1, f_2, \sigma_2, g, \tau, G$$

be a curve segment with parameter  $X_j$  over  $t$  on  $(\alpha_1, \alpha_2)$  where  $\alpha_1$  and  $\alpha_2$  are the elements of  $\mathbb{R}$  represented by the Thom encodings  $f_1, \sigma_1$  and  $f_2, \sigma_2$ .

The curve segment

$$f_1, \sigma_1, f_2, \sigma_2, g, \tau, G$$

is *well-parametrized* if the s-a curve  $\gamma : (\alpha_1, \alpha_2) \rightarrow \mathbb{R}\langle \varepsilon \rangle^k$  defined by

$$\gamma(x_j) = \left( \frac{g_1(t, x_j, u(x_j))}{g_0(t, x_j, u(x_j))}, \dots, \frac{g_k(t, x_j, u(x_j))}{g_0(t, x_j, u(x_j))} \right)$$

is well-parametrized, where  $u : (\alpha_1, \alpha_2) \rightarrow \mathbb{R}$  maps each  $x_j \in (\alpha_1, \alpha_2)$  to the root of  $g(t, x_j, U)$  with Thom encoding  $\tau$ . This means that

$$\sum_{i=1}^k \left( \left( \frac{g_i(t, x_j, u(x_j))}{g_0(t, x_j, u(x_j))} \right)' \right)^2 \leq k,$$

where the derivative is taken with respect to  $x_j$ .

Example 8.5 is not a well-parametrized curve segment.

If a curve segment defined over  $\mathbb{R}\langle \varepsilon \rangle$  is well-parametrized, and represents a curve bounded over  $\mathbb{R}$ , then the image of the curve under the  $\lim_\varepsilon$  map can be easily described. The following proposition explains why this is true.

**Proposition 8.7.** Let  $(a(\varepsilon), b(\varepsilon)) \subset \mathbb{R}\langle \varepsilon \rangle$ ,  $a(\varepsilon), b(\varepsilon)$  bounded over  $\mathbb{R}$ ,  $r < j \leq k$ ,  $z(\varepsilon) \in \mathbb{R}\langle \varepsilon \rangle^r$ , and

$$\gamma(\varepsilon) =: (a(\varepsilon), b(\varepsilon)) \rightarrow \{z(\varepsilon)\} \times \mathbb{R}\langle \varepsilon \rangle^{k-r}$$

a s-a differentiable curve parametrized by  $X_j$  and bounded over  $\mathbb{R}$ . If  $\gamma(\varepsilon)$  is well-parametrized, then:

- (1) there exists a continuous extension of  $\gamma(\varepsilon)$  to a continuous, s-a curve,

$$\gamma(\varepsilon) =: [a(\varepsilon), b(\varepsilon)] \rightarrow \{z(\varepsilon)\} \times \mathbb{R}\langle \varepsilon \rangle^{k-r}$$

defined over the closed interval  $[a(\varepsilon), b(\varepsilon)]$ ;

- (2) for each  $x \in [\lim_\varepsilon(a(\varepsilon)), \lim_\varepsilon(b(\varepsilon))]$  and any  $x(\varepsilon) \in [a(\varepsilon), b(\varepsilon)]$  with  $\lim_\varepsilon(x(\varepsilon)) = x$ ,  $\gamma(x) := \lim_\varepsilon(\gamma(\varepsilon)(x)) = \lim_\varepsilon(\gamma(\varepsilon)(x(\varepsilon)))$ ;
- (3)  $\lim_\varepsilon(\gamma(\varepsilon)([a(\varepsilon), b(\varepsilon)])) = \gamma([\lim_\varepsilon(a(\varepsilon)), \lim_\varepsilon(b(\varepsilon))])$ ,

In other words, the graph of the s-a function  $\gamma(-) := \lim_\varepsilon(\gamma(\varepsilon)(-))$  is the image under  $\lim_\varepsilon$  of the graph of  $\gamma(\varepsilon)$ .

*Proof.* Since  $\gamma(\varepsilon)$  is bounded it follows that there exists a continuous extension of  $\gamma(\varepsilon)$  to the end points of the interval  $(a(\varepsilon), b(\varepsilon))$ . It also follows from the definition of being well-parametrized that  $\|\gamma(\varepsilon)'(x)\| \leq \sqrt{k}$  for all  $x \in (a(\varepsilon), b(\varepsilon))$ . By the s-a mean value theorem [2, Exercice 3.4] we have that for each  $x \in (a(\varepsilon), b(\varepsilon)) \cap \mathbb{R}$  and any  $x(\varepsilon) \in (a(\varepsilon), b(\varepsilon))$  with  $\lim_{\varepsilon}(x(\varepsilon)) = x$ ,

$$\|\gamma(\varepsilon)(x) - \gamma(\varepsilon)(x(\varepsilon))\| = \|\gamma(\varepsilon)'(w(\varepsilon))\| |x - x(\varepsilon)|,$$

for some  $w \in (x, x(\varepsilon))$  (assuming without loss of generality that  $x < x(\varepsilon)$ ). Taking the image under  $\lim_{\varepsilon}$  and noticing that  $\|\gamma(\varepsilon)'(w(\varepsilon))\|$  is bounded over  $\mathbb{R}$  by the previous observation, we obtain that

$$\lim_{\varepsilon}(\gamma(\varepsilon)(x)) = \lim_{\varepsilon}(\gamma(\varepsilon)(x(\varepsilon))),$$

proving (1). This implies that the function  $\gamma : (\lim_{\varepsilon}(a(\varepsilon)), \lim_{\varepsilon}(b(\varepsilon))) \rightarrow \mathbb{R}^k$  defined by  $\gamma(x) = \lim_{\varepsilon}(\gamma(\varepsilon)(x))$  is a continuous, bounded (since  $\gamma(\varepsilon)$  is bounded over  $\mathbb{R}$ ) s-a function, and hence can be extended to a continuous, bounded s-a function on the closed interval  $[\lim_{\varepsilon}(a(\varepsilon)), \lim_{\varepsilon}(b(\varepsilon))]$ . Moreover, it is clear that  $\gamma(\lim_{\varepsilon}(a(\varepsilon))) = \lim_{\varepsilon}(\gamma(\varepsilon)(a(\varepsilon)))$  and  $\gamma(\lim_{\varepsilon}(b(\varepsilon))) = \lim_{\varepsilon}(\gamma(\varepsilon)(b(\varepsilon)))$ , since

$$\gamma(\lim_{\varepsilon}(a(\varepsilon))), \gamma(\lim_{\varepsilon}(b(\varepsilon))) \in \overline{\gamma((\lim_{\varepsilon}(a(\varepsilon)), \lim_{\varepsilon}(b(\varepsilon))))} = \lim_{\varepsilon}(\gamma(\varepsilon)([a(\varepsilon), b(\varepsilon)])).$$

It is then clear that (2) follows.  $\square$

A s-a curve is in general not well-parametrized. However, subdividing if necessary the curve into several pieces, it is possible to choose for each such piece a parametrizing coordinate which makes the piece well-parametrized. This is what we do in Algorithm 8 (Reparametrization of a Curve).

**ALGORITHM 8. [Reparametrization of a Curve]**

INPUT. (1)  $t \in \mathbb{R}^m$  represented by a triangular Thom encoding  $\mathcal{F}, \sigma$ ,  
 (2) a bounded curve  $S$  represented by a curve segment,

$$f_1, \sigma_1, f_2, \sigma_2, g, \tau, G$$

with parameter  $X_1$  in  $\mathbb{R}^k$  over  $t$  on  $(a, b)$ .

All the polynomials in the input have coefficients in  $\mathbb{D}$ .

OUTPUT. (1) A finite set  $\mathcal{V} = \{v_1, \dots, v_{N-1}\}$ , of real univariate representations over  $(t, c_i)$  where each  $c_i$  is represented by a Thom encoding over  $t$  fixing  $X_{m(i)}$ .  
 (2) A finite set  $\mathcal{W} = \{w_1, \dots, w_N\}$ , of curve segments with  $w_i$  parametrized by  $X_{\ell(i)}$ .  
 Moreover, the union of the curves represented by  $\mathcal{W}$ , and the points represented by  $\mathcal{V}$  define a partition of  $S$ .

COMPLEXITY If the polynomials occurring in the input have degrees bounded by  $D$ , then the complexity of the algorithm is bounded by  $k^{O(1)} D^{O(m)}$ .

PROCEDURE.

Step 1. Let  $g_1(X_1, T) = X_1 g_0(X_1, T)$ , and for each  $i, 1 \leq i \leq k$ , let

$$F_i := \left( \frac{\partial g}{\partial T} \right) \left( \frac{\partial g_i}{\partial X_1} g_0 - g_i \frac{\partial g_0}{\partial X_1} \right) - \left( \frac{\partial g_i}{\partial T} g_0 - g_i \frac{\partial g_0}{\partial T} \right) \left( \frac{\partial g}{\partial X_1} \right)$$



(which is proportional to the projection on the  $i$ -th coordinate of the tangent vector to the input curve by the chain rule) and

$$G_i := kF_i^2 - \sum_{j=1}^k F_j^2.$$

Step 2. Computing  $\text{RElim}_T(G_i, g)$ ,  $1 \leq i \leq k$ , using [2, Algorithm 11.19 (Restricted Elimination)], obtain a family  $\mathcal{L}$  of polynomials in the ring  $\mathbb{D}[T_1, \dots, T_m, X_1]$ . Subdivide  $(a, b)$  in a finite union of points and intervals over which the signs of the polynomials in  $\mathcal{L}$  are fixed using [2, Algorithm 12.23 (Triangular Sampling Points)] and get  $a = c_1 < \dots < c_L = b$ , where each  $c_j$  is represented by a Thom encoding  $(C_j, \sigma_j)$  over  $t \in \mathbb{R}^m$ , such that for each  $j$ ,  $1 \leq j \leq L$ , there exists an  $\ell(j)$ ,  $1 \leq \ell(j) \leq k$ , such that for all  $x_1 \in (c_{j-1}, c_j)$ ,  $G_{\ell(j)}(t, x_1, u(x_1)) \geq 0$ , denoting by  $u(x_1)$  the root of  $g(t, x_1, U)$  with Thom encoding  $\tau$ . For each  $j$  fix an  $\ell(j)$  satisfying this property.

Step 3. For each  $j$ ,  $1 \leq j \leq L$ , reparametrize the segment of the input curve over the interval  $(c_{j-1}, c_j)$  using the coordinate  $X_{\ell(j)}$ . Suppose without loss of generality from here on that  $\ell(j) = 2$ .

Step 3 a). Set

$$H := g^2 + (X_2 \cdot g_0(T, X_1, U) - g_2(T, X_1, U))^2 \in \mathbb{D}[T, X_1, X_2, U].$$

Note that  $\text{Zer}(H(t, -), \mathbb{R}^3)$  is a curve bounded over  $\mathbb{R}$  (by assumption on the input). Call Algorithm 1 (Curve Segments) with input the polynomial  $H$ , and the triangular system  $\mathcal{F}, \sigma$ , noticing that  $X_2$  is now the parameter. Let  $\mathcal{D}_i$  (respectively,  $\mathcal{C}_i$ ) be the set of distinguished points (respectively, curves) output by Algorithm 1.

Step 3 b). For each element

$$(h(T, X_2, V), \sigma_h, H(T, X_2, V)) \in \mathcal{D}_i,$$

where

$$H(T, X_2, V) = (h_0(T, X_2, V), h_1(T, X_2, V), h_2(T, X_2, V)),$$

use [2, Algorithm 12.19 (Triangular Sign Determination)] to check if the point  $(x_1, x_2, u)$  represented by  $(h, \sigma_h, (h_0, h_1, X_2 h_0, h_2))$  over  $t$ , coincides with

$$(x_1, \frac{g_2(t, x_1, u(x_1))}{g_0(t, x_1, u(x_1))}, u(x_1)).$$

Retain only the element

$$(h(T, X_2, V), \sigma_h, H(T, X_2, V)) \in \mathcal{D}_i$$

for which this is the case, and add to the set  $\mathcal{V}$  the real univariate representation  $u = (h, \sigma_h, G_H)$  (see Notation 4.6) representing a point  $v_h \in \mathbb{R}^k$ , with parameter  $X_2$  over  $t$ .

Step 3 c). For each element

$$(f_1(T, V), \sigma_1, f_2(T, V), \sigma_2, h(T, X_2, V), \sigma_h, H(T, X_2, V)) \in \mathcal{C}_i,$$

where

$$H(T, X_2, V) = (h_0(T, X_2, V), h_1(T, X_2, V), h_2(T, X_2, V)),$$

use [2, Algorithm 12.19 (Triangular Sign Determination)] to check if the point  $(x_1, x_2, u)$  represented by

$$h(T, X_2, V), \sigma_h, (h_0, h_1, X_2 h_0, h_2)$$

over  $t$ , coincides with

$$(x_1, \frac{g_2(t, x_1, u(x_1))}{g_0(t, x_1, u(x_1))}, u(x_1))$$

for  $x_2 = (v_1 + v_2)/2$  where  $v_1, v_2$  are represented by  $(f_1, \sigma_1)$  and  $(f_2, \sigma_2)$  respectively. Retain only the element of  $\mathcal{C}_i$  for which this is the case, and add to the set  $\mathcal{W}$  the curve segment

$$(f_1, \sigma_1, f_2, \sigma_2, h, \sigma_h, G_H)$$

with parameter  $X_2$  over  $t$  (see Notation 4.6).

PROOF OF CORRECTNESS. Let

$$(f_1, \sigma_1, f_2, \sigma_2, g, \tau, G)$$

be a curve segment parametrized by  $X_1$  over  $t$  representing the curve  $\gamma : (a, b) \rightarrow \mathbb{R}^k$ .

Let  $(c, d)$  be a sub-interval of  $(a, b)$  such that for every  $x_1 \in (a, b)$

$$G_\ell(t, x_1, u(x_1)) = kF_\ell^2(t, x_1, u(x_1)) - \sum_{j=1}^k F_j^2(t, x_1, u(x_1)) \geq 0. \quad (8.1)$$

(using the notation of Step 1 and Step 2).

This implies

$$\left| \frac{\partial \gamma_\ell}{\partial X_1} \right| \geq \frac{1}{\sqrt{k}},$$

and hence the mapping  $\gamma_\ell$  from  $(c, d)$  to  $(c', d')$  with  $c' = \gamma_\ell(c), d' = \gamma_\ell(d)$  is invertible. Defining  $\bar{\gamma}(x_\ell) = \gamma(\gamma_\ell^{-1}(x_\ell))$ ,  $\bar{\gamma}((c', d')) = \gamma((c, d))$  is well-parametrized by  $X_\ell$ .

Moreover, at each point  $x_1 \in (a, b)$  such a choice of  $\ell$  exists, since there must exist an  $\ell, 1 \leq \ell \leq k$  such that  $\left( \frac{\partial \gamma_\ell}{\partial X_1} \right)^2$  is at least the average value  $\frac{1}{k} \sum_{i=1}^k \left( \frac{\partial \gamma_i}{\partial X_1} \right)^2$ .

Notice also that for such a choice of  $\ell$  we have by the chain rule,

$$\sum_{i=1}^k \left( \frac{\partial \gamma_i}{\partial X_\ell} \right)^2 = \frac{\sum_{i=1}^k \left( \frac{\partial \gamma_i}{\partial X_1} \right)^2}{\left( \frac{\partial \gamma_\ell}{\partial X_1} \right)^2} \leq k. \quad (8.2)$$

In Step 2 of the algorithm we obtain a partition of the interval  $(a, b)$  into points and open intervals, such that over each sub-interval  $(c_{j-1}, c_j)$  of the partition, there exists an index  $\ell = \ell(j)$  such that (8.1) is satisfied at each point  $v \in (c_{j-1}, c_j)$ , and the curve segment over this interval is well-parametrized by  $X_\ell$  by (8.2).

Each curve segment corresponding to elements of  $\mathcal{V}$  output by the algorithm is thus well-parametrized. The remaining property of the output is a consequence of the correctness of Algorithm 1 (Curve Segments), and [2, Algorithm 12.19 (Triangular Sign Determination)].  $\square$

COMPLEXITY ANALYSIS. Let  $D$  be a bound on the degrees of the polynomials in the input. The complexity of Steps 1 and 2 is bounded by  $k^{O(1)}D^{O(m)}$  from the complexity of [2, Algorithm 11.19 (Restricted Elimination)], and [2, Algorithm 12.23 (Triangular Sample Points)], noting that the number of polynomials in  $\mathcal{L}$  is bounded by  $k^{O(1)}D^{O(m)}$ .

In Steps 3-4 the Algorithm 1 (Curve Segments) and [2, Algorithm 12.19 (Triangular Sign Determination)] are both called with a constant number of variables in the input. Using the complexity analysis of these algorithms, the total complexity is bounded by  $k^{O(1)}D^{O(m)}$ .  $\square$

8.2.2. *Limit of a curve.* We are now ready to describe Algorithm 4 (Limit of a Curve).

#### Description of Algorithm 4 (Limit of a Curve)

The algorithm proceeds by reparametrizing the curve and computing the limit of the well-parametrized curve segments so obtained, as explained below. Its precise input and output appear in Section 6.2.

##### PROCEDURE

Step 1. Let  $T = (T_1, \dots, T_m)$ ,  $X' = (X_1, \dots, X_r)$ . Call a slight variant of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], computing pseudo-reductions of the intermediate computations modulo  $\mathcal{F}$  (using Proposition 8.4), with input

$$\sum_{A \in \mathcal{H}(\varepsilon)} A^2 \in D[\varepsilon, T, X']$$

and parameters  $\varepsilon, T$ , and output the set  $\mathcal{U}_\varepsilon$  of parametrized univariate representations with variable  $U$ .

For every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{U}(\varepsilon)$ , use [2, Algorithm 12.20 (Triangular Thom Encoding)] with input the triangular system  $(\mathcal{F}, h(\varepsilon))$  to compute the Thom encodings of the real roots of  $h(\varepsilon)(y, U)$ . If

$$\mathcal{H}(\varepsilon) = (h_{[1]}, \dots, h_{[r]})$$

with  $h_{[i]} \in D[T, X_1, \dots, X_i]$  substitute the variables  $X'$  in

$$\bigcup_{0, \dots, r} \text{Der}_{X_i}(h_{[i]})$$

using  $H(\varepsilon)$  by (Notation 4.5) and define a family  $\mathcal{A}$  of polynomials in  $\varepsilon, T, U$ . Using [2, Algorithm 12. (Triangular Sign Determination)], compute the signs of the polynomials of  $\mathcal{A}$  at the roots of  $h(\varepsilon)(y, U)$ . Comparing the Thom encodings, identify a specific  $(h(\varepsilon), \tau(\varepsilon), H(\varepsilon))$  representing  $z(\varepsilon)$  over  $t$ .

Then apply Algorithm 3 (Limit of a Bounded Point) with input

$$(h(\varepsilon), \tau(\varepsilon), H(\varepsilon))$$

representing  $z(\varepsilon)$  over  $t$  to obtain a real univariate representation  $p_z, \rho_z, P_z$  representing  $z$  over  $t$ .

Step 2. Using Algorithm 8 (Reparametrization of a Curve) reparametrize the input curve segment.

Step 3. For every well-parametrized curve segment  $S(\varepsilon)$  computed in Step 2, and represented by

$$(f(\varepsilon)_1, \sigma(\varepsilon)_1, f(\varepsilon)_2, \sigma(\varepsilon)_2, g(\varepsilon), \tau(\varepsilon), G(\varepsilon)),$$

do the following.

First reorder the variables to ensure that the parameter of  $S(\varepsilon)$  is  $X_{r+1}$ .

Then compute a description of  $\lim_\varepsilon(S(\varepsilon))$ . This process is going to generate a finite list of open intervals and points above which the representation of the restriction of the curve  $\lim_\varepsilon(S(\varepsilon))$  by a curve segment is fixed. This is done as follows.

Step 3 a). Denote by  $\alpha(\varepsilon)_1$  the element of  $R\langle\varepsilon\rangle$  represented by

$$f(\varepsilon)_1(T, X', X_{r+1}), \sigma(\varepsilon)_1$$

over  $(t, z(\varepsilon))$ .

Call a slight variant of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], computing pseudo-reduction of the intermediate computations modulo  $\mathcal{F}$  of the output modulo  $\mathcal{F}$  (using Proposition 8.4), with input

$$\sum_{A \in \mathcal{H}(\varepsilon)} A^2 + f(\varepsilon)_1(T, X', X_{r+1})^2 \in D[\varepsilon, T, X', X_{r+1}]$$

and parameters  $\varepsilon, T$ , and output a set  $\mathcal{U}'_\varepsilon$  of parametrized univariate representations with variable  $U$ .

For every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{U}'_\varepsilon$ , use [2, Algorithm 12.20 (Triangular Thom Encoding)] with input the triangular system  $(\mathcal{F}, h(\varepsilon))$  to compute the Thom encodings of the real roots of  $h(\varepsilon)(y, U)$ .

If

$$\mathcal{H}(\varepsilon) = (h_{[1]}, \dots, h_{[r]})$$

with  $h_{[i]} \in D[T, X_1, \dots, X_i]$  substitute the variables  $X', X_{r+1}$  in

$$\text{Der}_{X_{r+1}}(f(\varepsilon)_1(T, X', X_{r+1}), X_{r+1} \cup \bigcup_{1, \dots, r} \text{Der}_{X_i}(h_{[i]}))$$

using Notation 4.5 and define a family  $\mathcal{B}$  of polynomials in  $\varepsilon, T, U$ . Using [2, Algorithm 12. (Triangular Sign Determination)], compute the signs of the polynomials of  $\mathcal{B}$  at the roots of  $h(\varepsilon)(y, U)$ . Comparing the Thom encodings, identify a specific  $(h(\varepsilon), \tau(\varepsilon), H(\varepsilon))$  representing  $(z(\varepsilon), \alpha(\varepsilon)_1)$  over  $t$ .

Then apply Algorithm 3 (Limit of a Bounded Point) with input

$$(h(\varepsilon), \tau(\varepsilon), H(\varepsilon))$$

representing  $(z(\varepsilon), \alpha(\varepsilon)_1)$  over  $t$  to obtain a quasi-monic real univariate representation  $p_{z, \alpha_1}, \rho_{z, \alpha_1}, P_{z, \alpha_1}$  representing  $(z, \alpha_1)$  over  $t$  with  $\alpha_1 = \lim_\varepsilon(\alpha(\varepsilon)_1)$ . Obtain a Thom encoding over  $t$ , of  $\alpha_1$  using [2, Algorithm 15.1 (Projection)].

Similarly, for  $\alpha(\varepsilon)_2$  the element of  $R\langle\varepsilon\rangle$  represented by

$$f(\varepsilon)_2(T, X', X_{r+1}), \sigma(\varepsilon)_2$$

over  $(t, z(\varepsilon))$ , compute a Thom encoding over  $t$ , of  $\alpha_2 = \lim_\varepsilon(\alpha(\varepsilon)_2)$ .

- Step 3 b). Perform a slight variant of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], computing pseudo-reductions of intermediate computations modulo  $\mathcal{F}$  of the output modulo  $\mathcal{F}$  (using Proposition 8.4), with input

$$\sum_{A \in \mathcal{H}(\varepsilon)} A^2 + g(\varepsilon)(T, X', X_{r+1}, V)^2 \in D[\varepsilon, T, X', X_{r+1}, U]$$

with parameters  $\varepsilon, T, X_{r+1}$  and output a set  $\mathcal{V}(\varepsilon)$  of parametrized univariate representations with parameter  $\varepsilon, T, X_{r+1}$  and variable  $V$ . Denote by  $\Theta(\varepsilon)$  the set of polynomials  $\theta(\varepsilon)$  such that there exists  $\Theta(\varepsilon)$  with  $(\theta(\varepsilon), \Theta(\varepsilon)) \in \mathcal{V}(\varepsilon)$ . Note that  $\theta(\varepsilon) \in D[\varepsilon, T, X_{r+1}, V]$ .

- Step 3 c). Compute the family of coefficients  $\mathcal{C} \subset D[T, X_{r+1}]$  of the polynomials  $\theta(\varepsilon) \in \Theta(\varepsilon)$  considered as elements of  $D[T, X_{r+1}][\varepsilon, V]$  and the list  $\mathcal{L} \subset \{= 0, \neq 0\}^{\mathcal{C}}$  of non-empty conditions  $= 0, \neq 0$  satisfied by  $\mathcal{C}$  in  $\mathbb{R}$  using [2, Algorithm 12.23 (Triangular Sample Points)]. Note that for every  $x_{r+1}$  in the realization of  $\tau \in \mathcal{L}$ , the orders in  $\varepsilon$  of the coefficients of the polynomials in  $\Theta(\varepsilon)(t, x_{r+1}) \subset D[\varepsilon, V]$  are fixed. For every  $\theta(\varepsilon) \in \Theta(\varepsilon)$  we denote by  $o(\theta(\varepsilon), \tau)$  the minimal order in  $\varepsilon$  of the coefficients of  $\theta(\varepsilon)(t, x_{r+1})$  on the realization of  $\tau$  and by  $\Theta_\tau \subset D[T, X_{r+1}, V]$  the set of polynomials obtained by substituting 0 for  $\varepsilon$  in  $\varepsilon^{-o(\theta(\varepsilon), \tau)}\theta(\varepsilon)$ .

- Step 3 d). Define

$$\Theta = \bigcup_{\tau \in \mathcal{L}} \Theta_\tau \subset D[T, X_{r+1}, V].$$

Compute

$$\mathcal{E} = \mathcal{C} \cup \bigcup_{\theta \in \Theta} \text{RElim}_V(\theta, \text{Der}(\theta)) \subset D[T, X_{r+1}]$$

using [2, Algorithm 11.19 (Restricted Elimination)], so that the Thom encodings of the real roots of  $\theta(t, x_{r+1}, V)$  are fixed when  $x_{r+1}$  varies in an open interval defined by the roots of the polynomials  $\mathcal{E}(t)$ .

- Step 3 e). Compute using [2, Algorithm 12.19 (Triangular Sign Determination)] the Thom encodings of the real roots of the polynomials in  $\mathcal{E}(t)$ , and the ordered list  $c_1 < \dots < c_{h-1}$  of the roots of the polynomials in  $\mathcal{E}(t)$  in the interval  $(c_0, c_h)$ , with  $c_0 = \alpha_1, c_h = \alpha_2$ . Denote by  $C_j, \rho_j$  a polynomial in  $\mathcal{E}(t)$  and a Thom encoding representing  $c_j$ .
- Step 3 f). For every  $j$  from 1 to  $h-1$ , and for every  $\theta \in \Theta$ , determine using [2, Algorithm 12.19 (Triangular Sign Determination)], the Thom encoding

$$\theta(t, c_j, V), \tau_j$$

of a root  $v_j$  such that  $v_j = \lim_{\varepsilon}(v(\varepsilon))$ , where  $v(\varepsilon)$  is the root of  $\theta(\varepsilon)(t, c_j, V)$  with Thom encoding  $\tau(\varepsilon)$ . The multiplicity  $\mu_j$  of the root  $v_j$  is determined by  $\tau_j$ .

- Step 3 g). For every  $j$  from 1 to  $h$ , define  $I = (c_{j-1}, c_j)$ . For every  $\theta \in \Theta$  determine, using [2, Algorithm 12.19 (Triangular Sign Determination)] the Thom encoding  $\theta_I(t, x_{r+1}, V), \tau_I$  of a root  $v_I(x_{r+1})$ , of multiplicity  $\mu_I$  such that for every  $x_{r+1} \in I$ ,  $v_I(x_{r+1}) = \lim_{\varepsilon}(v(\varepsilon))$  where  $v(\varepsilon)$  is the root of  $\theta(\varepsilon)(t, x_{r+1}, V)$  with Thom encoding  $\tau(\varepsilon)$ . The multiplicity  $\mu_I$  of the root  $v_I(x_{r+1})$  is determined by  $\tau_I$ .

- Step 3 h). Given  $(\theta(\varepsilon), \Theta(\varepsilon))$  in  $\mathcal{U}(\varepsilon)$  denote by  $(g_{\Theta(\varepsilon)}, G_{\Theta(\varepsilon)})$  the  $k - r + 1$ -tuple of polynomials obtained by substituting in  $(g(\varepsilon), G(\varepsilon))$  the variables  $X', U$  by  $F(\varepsilon)$  (see Notation 4.5). Denote by  $\mathcal{V}'(\varepsilon) \subset \mathcal{D}[\varepsilon, T, X_j, V]$  the set of  $k - r + 1$ -tuples of polynomials  $(g_{\Theta(\varepsilon)}, G_{\Theta(\varepsilon)})$ .
- Step 3 i). For every  $j$  from 1 to  $h - 1$  and every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{V}'(\varepsilon)$ , with  $H(\varepsilon) = (h(\varepsilon)_0, h(\varepsilon)_{r+2}, \dots, h(\varepsilon)_k)$  determine the order in  $\varepsilon$  of

$$h_\varepsilon(t, c_j, v_j), h(\varepsilon)_i(t, c_j, v_j).$$

This is done by determining the signs of the coefficient  $h_\ell, h_{i,\ell}$  of  $\varepsilon^\ell$  in  $h(t, c_j, v_j), h_i(t, c_j, v_j)$  using [2, Algorithm 12.19 (Triangular Sign Determination)]. Retain those  $(h(\varepsilon), H(\varepsilon))$  such that  $o(h(\varepsilon)_0) \leq o(h(\varepsilon)_i)$  for all  $i$  from  $r + 2$  to  $k$  and replace  $\varepsilon$  by 0 in

$$(\varepsilon^{-o(h_\varepsilon)} h(\varepsilon), \varepsilon^{-o(h(\varepsilon)_0)} H(\varepsilon)),$$

which defines a set  $\mathcal{H}_j$ . Inspecting every  $(h, H) \in \mathcal{H}_j$ , determine, using [2, Algorithm 12.19 (Triangular Sign Determination)], a  $k - r + 1$ -tuple  $(h_j, H_j)$  with the following property. Let  $d_j$  be the point represented by the real univariate representation

$$(h_j(T, X_{r+1}, V), \tau_j, H_j^{(\mu_j-1)}(T, X_{r+1}, V))$$

over  $t, u$ . The image under  $\lim_\varepsilon$  of the point of  $S(\varepsilon)$  with  $X_{r+1}$ -coordinate  $(c_j)$  is  $(z, c_j, d_j)$ .

- Step 3 j). For every  $j$  from 1 to  $h$  define  $I = (c_{j-1}, c_j)$ . For every  $(h(\varepsilon), H(\varepsilon)) \in \mathcal{V}'(\varepsilon)$ , with  $H(\varepsilon) = (h(\varepsilon)_0, h(\varepsilon)_{r+2}, \dots, h(\varepsilon)_k)$  subdivide  $I$  so that the order in  $\varepsilon$  of  $h(\varepsilon)(t, c_j, v_j)$  and  $h_i(\varepsilon)(t, x_{r+1}, v_I(x_{r+1}))$  is fixed. This is done by computing

$$\mathcal{E}_I = \bigcup_{\theta \in \Theta, (h, H(\varepsilon)) \in \mathcal{V}'(\varepsilon), 0 \leq \ell \leq \deg_\varepsilon h_i} \text{RElim}_V(\theta, h_\ell) \subset \mathcal{D}[T, X_{r+1}],$$

and

$$\mathcal{E}_{I,i} = \bigcup_{\theta \in \Theta, (h, H(\varepsilon)) \in \mathcal{V}'(\varepsilon), 0 \leq \ell \leq \deg_\varepsilon h_i} \text{RElim}_V(\theta, h_{i,\ell}) \subset \mathcal{D}[T, X_{r+1}],$$

using [2, Algorithm 11.19 (Restricted Elimination)].

Defining

$$\mathcal{E}'_I = \mathcal{E}_I \cup \bigcup_{i \in \{0, r+2, \dots, k\}} \mathcal{E}_{I,i},$$

compute the Thom encodings of the roots of the polynomials in  $\mathcal{E}'_I(t)$ , using [2, Algorithm 12.19 (Triangular Sign Determination)]. On each open interval  $J$  between two successive roots, the order in  $\varepsilon$ , denoted by  $o(h_\varepsilon), o(h(\varepsilon)_i)$  of the polynomials

$$h(\varepsilon)(t, x_{r+1}, v_J(x_{r+1})), h_i(\varepsilon)(t, x_{r+1}, v_J(x_{r+1}))$$

remains fixed.

Retain those  $(h(\varepsilon), H(\varepsilon))$  such that  $o(h(\varepsilon)_0) \leq o(h(\varepsilon)_i)$  for all  $i$  from  $r + 2$  to  $k$  and replace  $\varepsilon$  by 0 in  $\varepsilon^{-o(h(\varepsilon)_0)}(h, H(\varepsilon))$ , which defines a set  $\mathcal{H}_J$ . Inspecting every  $(h, H) \in \mathcal{H}_J$ , determine, using [2, Algorithm 12.19

(Triangular Sign Determination)], a  $k - r + 1$ -tuple  $(h_J, H_J)$  such that the point represented by

$$(h_J(t, x_{r+1}, v_I), H_J^{(\mu_J-1)}(t, x_{r+1}, v_I))$$

is the image under  $\lim_\varepsilon$  of the point of  $S(\varepsilon)$  with  $X_{r+1}$ -coordinate  $x_{r+1}$ , where  $\mu_J$  is the multiplicity of  $u_J(x_{r+1})$  as a root of  $h_J(x_{r+1}, V)$ .

Let  $w_J$  be the curve represented by the curve segment representation

$$h_I(T, X_{r+1}, U), \tau_j, H_J^{(\mu_J-1)}(T, X_{r+1}, U)$$

with parameter  $X_{r+1}$  over  $t, u$ .

Step 3 k). Let  $c_1 < \dots < c_{N-1}$  denote the set of all the elements of  $\mathbb{R}$  computed in Steps 2 d), and 2 i) above, and  $c_N = c$ . Re-index each  $v_j$  computed in Step 3 h), such that  $d_j$  lies above  $c_j$ . Similarly, re-index each  $w_I$  computed in Step 3 i) by some  $j$ ,  $1 \leq j \leq N$ , so that  $w_j$  lies above the interval  $(c_{j-1}, c_j)$ . Output the lists consisting of  $d_1, \dots, d_{N-1}$ , and  $w_1, \dots, w_N$ .

PROOF OF CORRECTNESS. Let  $\gamma(\varepsilon) : (\alpha(\varepsilon)_1, \alpha(\varepsilon)_2) \rightarrow \mathbb{R}\langle\varepsilon\rangle^k$  be the curve represented by a well-parametrized curve segment

$$f(\varepsilon)_1, \sigma(\varepsilon)_1, f(\varepsilon)_2, \sigma(\varepsilon)_2, g(\varepsilon), \tau(\varepsilon), G(\varepsilon)$$

computed in Step 2.

Let  $G : (\alpha_1, \alpha_2) \rightarrow \mathbb{R}^k$  be the curve whose image equals the image of  $\gamma(\varepsilon)$  under  $\lim_\varepsilon$ . Since the input curve segment is well-parametrized it follows from Proposition 8.7 that in order to compute for any  $x_1 \in (c_0, c_N)$ ,  $G(x_1)$  it suffices to compute  $\lim_\varepsilon \gamma(\varepsilon)(x_1)$ . The proof of correctness of the algorithm is then similar to the proof of correctness of Algorithm 3 (Limit of a Bounded Point).  $\square$

COMPLEXITY ANALYSIS. Let  $D$  be a bound on the degrees of all polynomials appearing in the input. We first bound the degrees in the various variables,  $\varepsilon, T, X', X_{r+1}, U, V$  of the polynomials computed in various steps of the algorithm. In Step 1, the degrees of the polynomials in  $\mathcal{U}(\varepsilon)$  are bounded as follows. The degrees in  $\varepsilon, U$  are bounded by  $D^{O(r)}$  by the complexity analysis of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] and the degrees in the  $T_i$  are bounded by  $D$ , because of the pseudo-reduction. Moreover, the complexity of this step is bounded by  $D^{O(m+r)}$  from the complexity of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)] and the complexity of pseudo-reduction (see Definition 4.2).

The degrees in  $\varepsilon, T_i, X', U$  in the output of Step 2 are all bounded by  $D^{O(1)}$  and the complexity of Step 2 is bounded by

$$(k - r)^{O(1)} D^{O(m+r)} = k^{O(1)} D^{O(m+r)}$$

using the complexity analysis of Algorithm 8 (Reparametrization of a Curve).

The degrees of the polynomials in Step 3 a are bounded as follows. In the output of the call to [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], the degrees in  $\varepsilon, U$  are bounded by  $D^{O(r)}$ , and the degrees in the  $T_i$  are bounded by  $D$ . Now, from the complexity analysis of Algorithm 3 (Limit of a Bounded Point) it follows that the degrees in the  $T_i$  of the polynomials output are bounded by  $D$  and those in  $\varepsilon, U$  are bounded by  $D^{O(r)}$ . Moreover, the complexity of Step 3 a is bounded by  $D^{O(m+r)}$  from the complexity of [2, Algorithm 12.18 (Parametrized

Bounded Algebraic Sampling)], the complexity of Algorithm 3 (Limit of a Bounded Point) and the complexity of pseudo-reduction (see Proposition 8.4).

The degrees of the polynomials in Step 3 b are bounded as follows. In the output of the call to [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], the degrees in  $\varepsilon, X_{r+1}, V$  are bounded by  $D^{O(r)}$ , and the degrees in the  $T_i$  are bounded by  $D$ . The complexity of Step 3 b is bounded by  $D^{O(m+r)}$  from the complexity of [2, Algorithm 12.18 (Parametrized Bounded Algebraic Sampling)], and the complexity of pseudo-reduction (see Definition 4.2).

The complexity of Step 3 c is bounded by  $D^{O(m+r)}$  using the degree bounds from the complexity analysis of the previous steps and the complexity of [2, Algorithm 12.23 (Triangular Sample Points)].

It now follows from the complexity analysis of [2, Algorithm 12.19 (Triangular Sign Determination)], [2, Algorithm 11.19 (Restricted Elimination)], and the degree estimates proved above that the complexity of the remaining steps are all bounded by  $k^{O(1)}D^{O(m+r)}$ . Thus, the complexity of the algorithm is bounded by  $k^{O(1)}D^{O(m+r)}$ .  $\square$

#### ACKNOWLEDGEMENT

We are very grateful to the anonymous referees of the paper for their numerous suggestions. We are particularly grateful to one of them for pointing out an error in a preliminary version.

#### REFERENCES

- [1] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets on a variety. *J. Amer. Math. Soc.*, 13(1):55–82, 2000. [1](#)
- [2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006 (second edition). [1](#), [2](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [11](#), [13](#), [14](#), [15](#), [19](#), [20](#), [22](#), [23](#), [24](#), [25](#), [26](#), [27](#), [29](#), [32](#), [33](#), [34](#), [35](#), [36](#), [37](#), [39](#), [40](#), [41](#), [42](#), [43](#), [44](#), [45](#), [46](#), [47](#)
- [3] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2011, online version posted on 3/08/2011, available at <http://perso.univ-rennes1.fr/marie-francoise.roy/>. [5](#), [6](#), [7](#), [9](#), [10](#), [15](#), [18](#), [19](#), [30](#), [31](#), [32](#)
- [4] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle (Second edition in english: Real Algebraic Geometry)*, volume 12 (36) of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin, 1987 (1998). [8](#), [12](#)
- [5] J. Canny. *The Complexity of Robot Motion Planning*. MIT Press, 1987. [1](#)
- [6] G. E. Collins. Quantifier elimination for real closed fields by cylindric algebraic decomposition. In *Second GI Conference on Automata Theory and Formal Languages*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183, Berlin, 1975. Springer-Verlag. [1](#)
- [7] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001. [34](#)
- [8] Mohab Safey el Din and Eric Schost. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete Comput. Geom.*, 45(1):181–220, 2010. [2](#), [6](#), [8](#)
- [9] L. Gournay and J. J. Risler. Construction of roadmaps of semi-algebraic sets. *Appl. Algebra Eng. Commun. Comput.*, 4(4):239–252, 1993. [1](#)
- [10] D. Grigoriev and N. Vorobjov. Counting connected components of a semi-algebraic set in subexponential time. *Comput. Complexity*, 2(2):133–186, 1992. [1](#)
- [11] D. Yu. Grigoriev, J. Heintz, M.-F. Roy, P. Solernó, and N.N. Vorobjov, Jr. Comptage des composantes connexes d’un ensemble semi-algébrique en temps simplement exponentiel. *C. R. Acad. Sci. Paris Sér. I Math.*, 311(13):879–882, 1990. [1](#)



- [12] J. Heintz, M.-F. Roy, and P. Solernò. Single exponential path finding in semi-algebraic sets ii: The general case. In Chandrajit L. Bajaj, editor, *Algebraic geometry and its applications*, pages 449–465. Springer-Verlag, 1994. Shreeram S. Abhyankar’s 60th birthday conference, 1990. [1](#)
- [13] Joos Heintz, Marie-Françoise Roy, and Pablo Solernó. Single exponential path finding in semialgebraic sets. I. The case of a regular bounded hypersurface. In *Applied algebra, algebraic algorithms and error-correcting codes (Tokyo, 1990)*, volume 508 of *Lecture Notes in Comput. Sci.*, pages 180–196. Springer, Berlin, 1991. [1](#)
- [14] J. Schwartz and M. Sharir. On the piano movers’ problem ii. general techniques for computing topological properties of real algebraic manifolds. *Adv. Appl. Math.*, 4:298–351, 1983. [1](#)
- [15] N. N. Vorobjov, Jr. and D. Yu. Grigoriev. Determination of the number of connected components of a semi-algebraic set in subexponential time. *Dokl. Akad. Nauk SSSR*, 314(5):1040–1043, 1990. [1](#)

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, IN 47907, USA  
*E-mail address:* `sbasu@math.purdue.edu`

IRMAR (URA CNRS 305) UNIVERSITÉ DE RENNES 1 CAMPUS DE BEAULIEU 35042 RENNES,  
 CEDEX FRANCE  
*E-mail address:* `marie-francoise.roy@univ-rennes1.fr`

SORBONNE UNIVERSITÉS, UPMC, UNIV. PARIS 06, UMR CNRS 7606, LIP6, INRIA PARIS-  
 ROCQUENCOURT CENTER POLSYS PROJECT, INSTITUT UNIVERSITAIRE DE FRANCE, FRANCE  
*E-mail address:* `Mohab.Safey@lip6.fr`

COMPUTER SCIENCE DEPARTMENT, THE UNIVERSITY OF WESTERN ONTARIO, LONDON, ON,  
 CANADA  
*E-mail address:* `eschost@uwo.ca`